USER ACCEPTANCE OF SYSTEMS FOR ARCHIVING AND SECURING DEGREE CERTIFICATES AND RELATED DOCUMENTS

Philisiwe Joyce Myeza

School of Management, IT and
Governance University of KwaZulu-Natal, Durban
Republic of South Africa

A thesis submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

Lead Supervisor: Prof. Jonathan Blackledge
Co-Supervisor: Prof. Brian McArthur

October 2019

ABSTRACT

Changing economic circumstances have led to the investigation of alternative solutions to economic problems. This has had an impact on communities who see academic qualifications as a solution to securing employment. With the increase in job opportunities requiring suitable qualifications, an increase in 'qualification competition' has occurred. This has resulted in academic qualifications being seen as a 'key' to securing employment. Unfortunately, such a perception has caused many individuals to pursue opportunities using 'quick fix' solutions and acquiring academic qualifications through breaches of security around these qualifications. Higher Education is one of the many sectors that is battling with security issues of this type. In South Africa alone, for the past few years, there has been a considerable increase in cases of persons who have been found to have faked either their senior certificates or university degrees, including doctorates. This is becoming a growing concern as it taints the image of the higher education sector in South Africa, and places at risk international relationshipsin higher education and beyond that the country has enjoyed over many years.

Many education sectors are based on security systems in which the basic data of a person's name and surname, for example, are retained when they graduateand the qualification they have legitimately received is recorded. This data is used when a re-print of a certificate is required. Though this method has been working well for some time, it has developed major flaws, in line with the sophistication of information and communications technology in general. This applies especially to the ability to edit e-versions of a certificate using image processing software. Thus, proper verification of the data captured in an e-version or hard-copy of a certificate (when reprinted, for example), represents an increasing risk, and, in some cases, results in a breach of security. Furthermore, some individuals have found ways to e-edit and print their own certificates, which look effectively identical to the authenticated certificates.

While the emerging trend in various sectors is to store all data using the appropriate technology tools as a security measure for protecting information, organizations are becoming exposed to cybercrimes. As a result, data security has increasingly become a cause for concern. What is most disturbing, is that computer security breaches have increased, and in many cases, shown to be the result of 'insider misuse and abuse' of the information security measures established by an organization. It is for this reason that the current study and the work reported in this thesis has been undertaken and involves a focus on understanding what causes users to accept and follow an organization's information systems security measures.

The study is informed by the Unified Theory of Acceptance and Use of Technology (UTAUT), as a framework to explore securing and archiving academic transcripts at the University of KwaZulu-Natal (UKZN). The results showed that the intention of the UKZN staff to use the system positively, relates to their performance expectancy, effort expectancy, social influence and facilitating conditions. The use of UTAUT in a mixed methods study within an academic environment assesses the existing measures of securing and archiving academic transcripts and identifies various weaknesses in the current system. Based on the findings of the study, the steganographic method is demonstrated and suggested as an improved method of securing and archiving academic certificates at UKZN.

The original contribution is an in-depth study at UKZN that answered the user acceptance research questions and demonstrated the practical application of the steganographic method in securing and archiving data.

DECLARATION

I Philisiwe Joyce Myeza declare that:

(i) The research reported in this dissertation, except where otherwise indicated, is my original work.

(ii) This dissertation has not been submitted previously or otherwise for any degree or examination at any other university.

(iii) This dissertation does not contain other person's data, pictures, graphs or other information, unless specifically acknowledged as sourced work from other persons.

(iv) This dissertation does not contain other person's writing, unless specifically acknowledged as sourced work from other researchers. Where other written sources have been quoted:

a. their words have been re-written but general information attributed to them has been referenced;

b. where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.

(vi) This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source has been properly detailed in the dissertation and in the References section.

Signed: …….

Signature:_____ Date: October, 2019

ACKNOWLEDGEMENTS

I would like to express my gratitude to the lead supervisor Professor Dr Jonathan Blackledge for believing in me and for all his advice and support.

I would also like to express my sincere thanks to Professor Brian McAthur, who was always positive and supportive of my study.

I would like to express my appreciation to Professor Mtapuri for his help with qualitative analysis.

PUBLICATIONS

Information Hiding with Data Diffusion using Convolutional Encoding for Superencryption (with J M Blackledge, P Tobin and C M Adolfo), International Journal for Pure and Applied Mathematics (Mathematica Aeterna), Longdom Publishing, Vol. 7, No. 4, 319-356, 2017.

https://www.longdom.org/archive/me-volume-7-issue-4-year-2017.html

Information Hiding using Convolutional Encoding (with J M Blackledge, P To- bin and C M Adolfo), ISSC2018, IEEE UK and Ireland Signal Processing Chapter, Queens University Belfast, 21-22 June 2018.

https://ieeexplore.ieee.org/document/8585354

LIST OF ACRONYMS

ASCII	American Standard Code for Information Interchange
AU	African Union
AV	Audio visual
BRICS	Brazil, Russia, India, China and South Africa
EP Theory	Explanation and PredictionTheory
IAU	International Association of Universities
ICS	Information communication services
ICT	Information communication technology
IPTC	International Press Telecommunications Council
IS	Information Systems
ISS	Information Systems Security
ITS	Information Technology systems
JSTOR	Journal Storage
METS	Metadata Encoding and Transmission Standards
NUC	Natal University College
OCLC	Online Computer Library Center
PMB	Pietermaritzburg
SAA	Student Academic Administration
SADC	Southern African Development Community
SAPPI	South African Pulp and Paper Industries
SAQA	South African Qualification Authority
TAM	Technology acceptance model
TRA	Theory of Reasoned Action

UDW	University of Durban-Westville
UKZN	University of KwaZulu-Natal
UNESCO	United Nations Educational Scientific and Cultural Organization
UTAUT	Unified Theory of Acceptance and Use of Technology

DEFINITION OF TERMS (SPECIFIC TO CRYPTOLOGY)

Asymmetric encryption

A cryptosystem in which encryption and decryption are performed using two different keys, called public and private key.

Authentication

A process used to verify the integrity of transmitted data.

Cipher

An algorithm used for encryption and decryption. It is data which is used to replace a piece of information with another object with an intention of concealing its meaning.

Ciphertext

The output of an encryption algorithm or the encrypted form of message data.

Code

A procedure for replacing a piece of information with another object with no intention to conceal meaning.

Confusion

A cryptographic technique that seeks to make the relationship between the plaintext and the ciphertext as complex as possible.

Covertext

The output associated with the application of a steganographic technique

Cryptography

The branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and authenticity of messages.

Cryptology

The study of secure communication which encompasses both cryptography and cryptanalysis.

Cryptanalysis

The branch of cryptology dealing with the breaking of a cipher to recover information or forging encrypted information that will be accepted as authentic.

Cryptosystem

Any system that is concerned with the encryption and decryption of information.

Decryption

The translation of encrypted text or data called ciphertext into original text or data called plaintext.
It is also known as deciphering.

Diffusion

A cryptographic technique that seeks to obscure the statistical characteristics of the plaintext by spreading out the influence of each individual plaintext elements over many ciphertext elements.

Digital Signature

An authentication mechanism that enables the creator of a message to attach a code which acts as a signature. The signature guarantees the source and integrity of the message.

Encryption

The conversion of plaintext or data into an unintelligible form by means of a public or private algorithm from which the plaintext can be recovered by decryption. It is also called enciphering.

Plaintext

The input to an encryption function or the output to a decryption function.

Private Key

One of the two keys used in an asymmetric encryption system. For secure communication, the private key should only be known to its user.

Public Key

One of the two keys used in an asymmetric encryption system. The public key is made public and is used in conjunction with a corresponding private key.

Secret Key

The key is used in a symmetric encryption system. Both participants must share the same key which remains a secret to protect the communication.

Steganography

The technique associated with hiding encrypted data in host data.

Stegotext

The host data used to hide plaintext or ciphertext.

Symmetric Encryption

A cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

CONTENTS

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

BACKGROUND

1.1 Introduction

The growing trends of academic fraud in South Africa are a cause for concern. Reports in reputable South African national newspapers of high-profile cases involving academic fraud and misrepresentation of qualifications have been on the rise (Du Plessis et al., 2015). South Africa is regarded as a developing country and a leading economy on the continent (Du Plessis et al., 2015). It is a member state of a number of common interest international groups. Having experienced many years of isolation due to the political situation prior to democratisation, South Africa has had to adapt and play catch-up to the advanced practices and social, economic, educational and technological developments that have been adopted elsewhere in the world. This quest to achieve developmental parity is beset with many challenges, including social resistance or stagnation, a lack of political will, skills shortages, and technological and economic challenges. These challenges have been recognised by the United Nations, which classifies South Africa's economic conditions as indicating a developing economy (United Nations, 2013).

Despite all these challenges, South Africa commands a respectable reputation for the quality of its tertiary education. Graduates of the country's universities are accepted in professions in developed countries. This reputation has, however, been dented in recent years, as cases have emerged of people attempting to enter European countries with fraudulent South African documentation. This has had far-reaching consequences in that even educational certificates from South African institutions have become suspect, especially in Britain, where many young South African professionals go to seek work. According to Du Plessis et al. (2015), the reason false qualifications and educational fraud have become a worldwide problem, is that academic qualifications have gained in commercial value and are used to ensure access to employment. Qualifications are increasingly becoming indispensable for a number of occupations (Hallak & Poisson, 2007; Ineson, 2013). The rise of the Internet has also contributed to the spread of educational fraud and falsified degrees due to the accessibility of high-quality desktop printing (Du Plessis et al., 2015).

Du Plessis et al. (2015) state that despite increased collaboration among higher education institutions within regions, there are still major problems in the processes.

The internationalisation of higher education in Africa is accompanied by growing concern regarding the increase of fraud in the education and training landscape.

This is further supported by the "United Nations Educational Scientific and Cultural Organisation (UNESCO) and the African Union (AU)" (Eckstein, 2003 in Du Plessis et al. 2015, 5), which have stated that for any attempt at the improvement of access to quality education for all to be successful, the corruption that is evident in the running of the education sector has to be dealt with first. In recent times, there have been widely publicised cases published in local and national newspapers, of senior executives in the public sector having submitted fraudulent degrees or made false claims to certain educational qualifications. The South African Qualifications Authority (SAQA) reported on news24, which is an English language South African online news publication, that school leaving certificates are the most faked qualifications, at 41 percent of overall fraudulent academic certificates. Further to this, there is growing frustration among many innocent people who want to pursue studies elsewhere but, due to fraud in their home country, find that their applications are put on hold. SAQA undertook to deal with the problem by contracting North West University to undertake desktop research into current practices and policies with regard to the verification of academic certificates in different regions of the African continent (Du Plessis et al. 2015, 3).

This research, grounded in the Unified Theory of Acceptance and Use of Technology (UTAUT), will demonstrate and illustrate how the existing archiving and securing of academic certificates could be enhanced by adapting Blackledge's method, which will be illustrated and demonstrated on a researcher's academic certificate obtained at the University of KwaZulu-Natal (UKZN). The intention will be to introduce an alternative way of protecting and securing e-mode degree certificates and to ensure long term preservationof the original degree certificates.

When Professor Jonathan Blackledge was appointed Deputy Vice-Chancellor for Research in August 2014, the university library was within his portfolio of work, and his vision was to create an e-library (electronic library). It is during this period thatthe library migrated to a new system, called WorldShare Management Services, and became the first library to have adopted the system on the African continent.

The library director later saw an opportunity to implement a project to automate degree certificates. This project would combine the library's technology of digitisation with encryption technology and archiving.

"All information security measures try to address at least one of three goals which is protect the confidentiality of data, preserve the integrity of data, promote the availability of data for authorized use" (Merkow and Breithaupt 2014, 3). Though there are modern technological tools that are being implemented to address information security, it is important to ensure that employees implement measures to protect their information. A positive attitude towards security systems is developed by experience and knowing what to expect from the system. Since studies confirm that internal threats to the security of data exist, it is advisable for the organisation to communicate important information on security policies to employees and also to see to it that they are adhered to by all.

1.2 Research Problem

Changing economic circumstances encourage people to look for alternative solutions to economic problems (Obeng-Odoom, 2013). These changes, which are depreciating currency, the rising cost of food, and lack of employment opportunities for unskilled labour, have had an impact on communities, which increasingly see academic qualifications as a means of securing employment. This is demonstrated by the growing numbers of matriculated learners seeking entry to university. The huge demand for jobs requiring qualifications has led to more people acquiring qualifications, which has brought about an increase in competition amongst those that are qualified. This has resulted in academic qualifications being seen as a ticket to securing well-paid employment. While some have taken the route of registering for study, where possible, other individuals have seized the opportunity for a quick fix, fraudulently acquiring these academic qualifications. The result is a breach of security in academic qualifications.

In South Africa alone, the news about the cases of faking of senior certificates or university degrees has been on the rise. This is becoming a growing concern as it taints the image of the sector and places at risk the international relationships the country's higher education sector has enjoyed over many years. Over the years, organisations have implemented different advanced information systems security (ISS) measures in order to protect key assets. However, despite all the resources that might have been exploited to ensure that the security measures were intact, there were still reports of security breaches.

The literature suggests that, though computer security breaches are assumed to be the work of outsiders, such breaches have also been the result of failure to comply with internal policies and procedures of information systems security measures. While it might be impossible to eliminate security breaches altogether, the study will investigate the factors that affect the University of KwaZulu-Natal employee acceptance of information systems security measures by using UTAUT to explore employees' acceptance of such measures at UKZN. In particular, this study will further investigate the securing and archiving of degree certificates.

The current system used by the university is called Innerweb, which is the repository of documents that are only accessible to UKZN staff. The systems used for archiving and securing academic certificates are the Integrated Technology System (ITS) and Student Management System (SMS). The acceptance and use of the Innerweb, ITS and SMS as a security system will be assessed through questionnaires and interviews with purposefully selected stakeholders. The combined results of the questionnaires and interviews will lead to a clear picture as to user acceptance and use of the existing security measures for the securing and archiving of degree certificates.

1.3 Research Questions

The research questions are as follows:

1). To what extent do various factors influence user acceptance of information security systems measures for securing and archiving information at UKZN?

2). To what extent do University of KwaZulu-Natal employee perceptions regarding the information systems security measures at UKZN, affect their intention to use these measures?

3). To what extent do others' beliefs about the use of information systems security measures affect UKZN employee perceptions of and intentions to use these measures?

4). To what extent does the current system used to archive academic certificates at UKZN display problems related to employee perceptions of the university's information systems security measures?

1.4 Research Design and Methodology

The research project started by surveying the general opinions of staff on archiving and securing information using the existing archival system called Innerweb, and then focused on an investigation of the existing archival system for degree certificates at UKZN to highlight the constructs of information security. These constructs, together with a discussion of the issues of security of the academic degree certificates and how they have previously been secured, answered the research questions of the study. The process started with a general survey of the archival system used, called Innerweb, then moved to the qualitative questions for archiving and securing academic certificates. The staff members working from the departments responsible with information security at UKZN responded to semi-structured questions administered with an interview guide.

1.5 Research Design

Data was gathered using survey questions and interviews focusing on demographics and scales to measure the variables of the research drawn from UTAUT: performance expectancy, effort expectancy, social influence and facilitating conditions, with gender, age, experience and voluntariness of use as moderators. Semi-structured questions probed the securing and archiving of academic degrees.

1.5.1 Ethical Considerations

According to Miles and Huberman (1994, 5) “honesty and trust, privacy, anonymity and confidentiality, and informed consent, harm and risk, must be attended to before any data can be gathered from participants”. In this study, confidentiality had the potential to become a major concern due to the sensitivity of the information under study. The researcher ensured that, where a demonstration must be performed using a certificate, the researcher’s private certificate was used. The researcher is employed by UKZN. The gatekeeper’s letter of approval to conduct the study at UKZN has been obtained from the university’s registrar and an Ethical Clearance approval letter has been received from the Ethics Committee (Appendix F).

1.5.2 Limitations of the Study

The study was conducted within the context of UKZN, where participants are involved in the management of degree certificates. Being a case study, certain unpredictable factors, like conditions, resources or people, are unique to the case. As a result, this study cannot be generalised to other institutions that may be similar to UKZN. However, it may be adapted with modifications. The purpose of the study is to evaluate the practice of securing degree certificates, using the framework of the UTAUT model. An assumption has been made that steganography might be useful or appropriate in the context of managing academic qualification documents.

1.5.3 Original Contribution of the Thesis

Secure and productive use of information technology is vital to the success of many businesses. Therefore, the results of this research will be utilised by managers in order to understand the factors that promote employee adoption and use of technology, as well as compliance with the organisation's information systems security measures, and the factors that promote positive attitudes towards technology. The ability to promote the adoption of information systems security measures may help organisations to better realise the internal benefits of technology. On the academic side, "Many studies have been conducted on information systems in order to develop and predict the factors that could influence the adoption of a technology" (Chin and Lin 2016, 3). However, this study uses a case study approach informed by the UTAUT model to examine the adoption of information systems security in the academic sector.

The study added new knowledge by firstly closing the gap which was highlighted by Siponen and Baskerville (2018) of a need for research which will yield theory-based empirical results leading to a practical solution. The results of this study confirmed that while many studies discuss human intervention as compromising security in organizations, complementary triangulation of qualitative and quantitative results revealed that employees at UKZN are familiar with the security meausres of the system which are in place, and have confirmed what will improve the security of academic certificates. The study further revealed that it is the security feature improvement that will help to protect sensitive data such as academic certificates. A demonstration of the use of the steganographic method in Chapter 9 provides a novel practical application of this method in securing digital documents.

1.5.4 Summary and Organisation of the Thesis

The thesis is organised as follows: Chapter 1 introduces the topic, outlines the necessary background and explains why the study is important to the Higher Education sector and to South Africa. The review of literature is in chapter 2, 3 and 4: Chapter 2 which is about digitisation and security of data. Chapter 3 discusses cryptology and its relevance in this context. Chapter 4 outlines the methodology of the study. Chapter 5 discusses information systems theories. Chapter 6 presents the results of the quantitative survey and in Chapter 7 the open-ended questions and the qualitative interviews results are presented. Chapter 8 uses the Mixed Method approach to compare and triangulate the findings from the quantitative and qualitative analyses. Chapter 9 demonstrates the steganocryptographic system security software. Finally, Chapter 10 provides the conclusions drawn and recommendations made from the research.

CHAPTER 2

LITERATURE REVIEW: DIGITISATION AND SECURITY

2.1 Introduction

Libraries all over the world are in a state of transition, as they work to become relevant to those they serve. This is seen in many ways, including the move to embrace technology in libraries. This involves the conversion of paper or print collections into electronic copies. One of the many advantages of an electronic library is that it appeals to the social-media generation, who want their information to be delivered online, anytime, anywhere, with no physical contact with library or information centre staff. This new generation has created a shift in how libraries shape their agenda. This shift has seen libraries redefine their role and move away from what could be regarded as a traditional role. The digitisation of physical print collections and the embracing of born-digital items, like e-books, have been on the agenda for quite some time.

As conversion of print into digital is embraced, the act of digitisation will not only allow for the digital storing of textbooks but will also play a key role in the safeguarding of other important documents across the university. A university's e- library could therefore act as a digital archive for other documents, such as degree certificates. It is therefore important to pay special attention to the role of security in digital libraries. The next section will focus on the issues surrounding security and computer security, and further unpack the reasons that libraries and special collections are making the move to digitisation. A conclusion will be drawn as to how the security of digital material is critical to redefining the role of libraries.

2.2 Security

"The strength of any secure document is in the combination of security features used to protect it" (Vorster 2014, 2). South Africa has an authenticated company called Sappi, which is responsible for the security of the print paper used for certificates, cheques and passports, while bank notes are imported from Europe. Although Sappi is the only South African company known to have produced a product that can withstand forgery, counterfeiting and fraud, it has faced some security challenges. One of the biggest challenges is the emergence of sophisticated fraudsters who are able to reproduce high quality digital printing. However, Sappi's watermark and UV inks are features which cannot yet be reproduced.

Paper security alone has its security challenges. It is noted that though the security of the paper used for highly confidential activities remains strong, there have been outsiders who have tried to produce products that may look similar but are fraudulent. The bank industry remains on high alert although there have been no alarming reported incidents. However, within the Higher Education sector, there have been a number of reports of fraudulent activities related to degrees faked by outsiders. The local newspapers have reported various fraudulent activities surrounding matriculation and degree certificates, including the sale in 2012 of cloned UNISA certificates. Another story reported that 30% of South African degree certificates presented to employers in New Zealand were found to have been falsified (News24). It is therefore important to secure documents with features that are known to withstand cloning. Cryptography provides strong features that are difficult to clone, in both print and electronic form, namely, watermarks and UV links. Successful use of cryptography has been demonstrated in electronic banking and home affairs. The reported benefit of cryptography is that it can support online and offline verification, which allows internal quality control and proper verification of authenticity (Hoffman, 2016). While securing print and electronic paper using cryptography may be successful, it remains important to look at other potential sites of security breaches. The next section will consider computer security, which may be vulnerable to breaches of security (Zepke and Leach, 2011).

2.3 Computer Security

Fordyce (1982) outlines the case of a reputable company where a senior member of staff noticed an identity number of a staff member logged on while it was known that she/he was not working at the time. Upon investigation, it was discovered that the staff member in question had given her/his staff identity credentials to his/her minor to use. The child used the passwords to login and play games and also gave the passwords to his friends to use (Fordyce 1982, 10).

Cases like these alarm companies, organisations and institutions, as they suggest that some of the greatest threats to information security could come from within due to careless use of the system. This case highlights examples of personal behaviour in applying information technology security measures, which is caused by the lack of training for employees. It is also clear that this is not a technical information technology issue since the password was given voluntarily to a minor. While there are many similar cases, sadly, many remain undiscovered and thus unreported.

This fact highlights the importance of computer security in securing data, which if not done could cost organisations, companies or institutions, huge damage to reputation. There is a continued trend of reported cases of computer crimes in business magazines.

"If users are not willing to accept security measures the systems will not bring the full benefits of the technology to the organization" (Venkatesh and Davis 2000, 2), especially as the identified perpetrators of an online crime are often employees. Hence various methods should be identified that can be used to influence employee attitudes regarding adoption of information security measures. Some of those are formal training, gaining experience and knowing what to expect out of the system's security, which will increase the likelihood that users will have a positive attitude towards the security measures, as well as their repercussions. The creation of awareness campaigns in day-to-day practices could be useful as well. Companies need to apply "usability testing and techniques to secure systems and develop security models and mechanisms for user friendly systems" (Jones 2009, 7).

While it is important for organisations to invest in physical information technology security and training of staff on acceptable practices, especially since this has been known to positively influence technology acceptance, it is critical to first understand "the factors that affect employee acceptance of information systems security measures" (Jones 2009, 9). When analysing the risk of computer security, it is imperative to bring management on board. Fordyce (1982) divides risk into administrative, technical and physical risk. Threats to computer security may appear in the form of natural disaster, power failures or persons. Computer security specialists agree with various computer standards that operate internationally, that there needs to be a computer action plan which consists of various areas (Fordyce, 1982; Adekambi and Green, 2015). These are discussed in the following section.

2.3.1 Physical and Administrative Control

This kind of control is of access, both physical and electronic. The intention is to minimize the risk of loss of data. It is always advisable to have back-up measures in place for emergencies; however, effective monitoring is critical in security (Fordyce, 1982).

2.3.2 Training and Qualifications of Staff

Computer security evolves therefore it requires staff to keep abreast of the changes all the time. Occupational training should involve education in the security measures of staff employed by

the entity. It also requires facilitating a sense of taking ownership and responsibility in the profession (Adekambi and Green, 2015).

2.3.3 Software Security

The important aspect of security is the software as it carries out executive orders which could easily impose damage within a short space of time. Access requires a great deal of protection. Software security procedures must make provision for any unplanned tasks. Any unauthorized login should be prevented. Access to the production source library should be only to staff members who are tasked to work on programs. (Fordyce, 1982).

2.3.4 Data Integrity

Data integrity ensures that well-trained staff are capable of performing the tasks assigned to them and are familiar with the protection and procedure policies and implications thereof, of compromising inside information. (Adekambi and Green, 2015).

2.3.5 Communication Protection

Communication protection ensures that access, which may be gained to the system remotely, is within the accepted norms of the organisation, hence remote passwords provide the security required to identify anyone who may have had access. (Fordyce, 1982).

2.3.6 Post-processing procedures

Post-processing procedures ensure that all executed processes are monitored and that back-up of data takes place whenever necessary (Fordyce, 1982).

2.3.7 Interactive Controls

Internal controls require effective and efficient security, especially since they rely heavy on the integrity of the people employed to ensure the smooth functioning of the system. Proper training of employees is essential, and it may be necessary to do a background check of employees. Internal controls also involve the assurance that the system executes programs as expected. The security protection plan requires that all the eight areas discussed (physical and administrative control, training and qualification of staff, software security, data integrity, communication

protection, post-processing procedures and interactive controls) should function in a coherent way to ensure the effective and efficient functioning of the organisation. However, the decisionmakers need to be part of all the communication to ensure that the plan is successful. The next section will explore a critical aspect of security: information and communication (Fordyce, 1982).

2.4 Information and Communication Security

Information and communication technology (ICT) have a heavy impact on decision making in almost all organisations and plays a vital part in how knowledge is organised and processed.

With the arrival of the Internet, ICT has taken on a large role in information sharing and exchange. However, it should be noted that security infrastructure has to be effective and efficient in order to preserve and protect the integrity of information flowing across different channels. "Data transferred between different locations and recipients can be vulnerable to interception and modification by a capable and interested person" (Hallot 2008, 3); as a result, the application of secure infrastructure is an essential component in any organisation (Hallot, 2008). It is thus critical that organisations invest in effective security applications to protect the data of the organisation and look more deeply at how internal processes may pose security risks in order to ensure the threat is not within. It is for these reasons that this thesis considers user acceptance of technology. The focus on the next paragraph is going to discuss the process of preserving print paper in an electronic format (Adekambi and Green, 2015).

2.5 Why Digitise?

There are many reasons that lead organisations to consider digitising the print papers they consider to be valuable.

These vary from wanting to safeguard the print copies in case of fire, theft or flood, to a desire to expose print documents that are hidden from potential users in inaccessible storage. Draycott (2000, 165) states that the Wellcome Trust digitised its records for the following reasons: "…the strengths of the Medical Photographic Library lie in its unique resource of material, the expertise of its staff, and the rapidly growing usage. It has created the demand from the academic community for remote access; and that users experienced difficulty accessing the holdings with the system in place at the time" (Draycott 2000, 165). The nature of the information housed by the Trust is sensitive and required a careful control of security when

considering digitising for access. Though the Trust saw a need to digitise, the important task for the Trust was to ensure that access remains restricted to protect copyright. For these reasons, the digitization system had to be customised to protect access by having a device that will track who accessed and downloaded images. “Visible and invisible watermarks, identifying banners and information in the International Press Telecommunications Council header of image files are used to help the Medical Photographic Library and its users to track and identify images from the Wellcome Trusts collections” (Draycott 2000, 169). In addition, “electronic files supplied for reproduction or academic use contained transaction-based information in an invisible watermark that link the files with the relevant license information” (Draycott 2000, 170). The benefit of digitisation is that it offers flexibility, allowing customised solutions for particular digitised collections. The following section explores other benefits of digitisation (Fleischhauer, 2003) and (Kwon, 2011).

2.6 Benefits of Digitisation

Columbia University (2015) identifies the benefits of digital capture as: “Encouragement of scholarly use through the provision of enhanced resources in the form of widespread dissemination of unique collections which provides (Smith 1999, 12-13):

- increased and enriched use through the ability to search, manipulating images and text;
- enhanced intellectual control through creation of new finding aid and links to bibliographic records;
- enhanced use through improved quality of image, for example, improved legibility of faded or stained documents;
- creation of a virtual collection through the flexible integration and synthesis of a variety of formats or scattered materials in different locations.”

However, it must be mentioned that though there are many advantages of digitising, disadvantages also exist. Smith (1999) asserts that the first disadvantage is cost for conducting the entire project of digitization; secondly, the digital preservation storage space requires constant upgrade. Grimmelmann (2010) discusses some of the disadvantages that may arise out of the copyright ownership lawsuit. One example is the Google project to digitise all books. Despite all the challenges, digitisation will continue to offer improved accessibility for existing users, and therefore help attract new users who had previously been unaware of the print resources.

As noted, the UKZN library, where "the present author is employed in the capacity of library director, decided to embark on a drive to become an e-library. This was marked by the implementation of WorldShare Management Services, a product of OCLC. This provides the library with access to almost all the resources published worldwide. The advantage of the implementation of the system is that, despite financial constraints that forced the library to cut a number of full-text databases, library patrons they had previously been able to access almost all the collections they were used to accessing. However, the library had to implement a pay-as-you-go system for those full-text articles for which there was no subscriber access. This method has proved to be effective for academics and patrons, while it also represented cost- saving for the library.

Digitisation is being embraced all over the world. Recently, the researcher in the capacity of Library Director, visited first-world libraries and learned that they are embracing the digitisation of print copies to make them available to the world. What this means for future libraries, is that traditional libraries are no longer relevant to the patrons they serve. This means libraries must adapt to the changing world and focus on what is currently trending in the information world. It is also within these highlighted changes that libraries must begin to take a proactive rather than reactive role. Libraries must identify the areas where they can have an impact in order to remain relevant. It is for these reasons that the researcher has identified a library as a place that fully embraces digital archiving that, if paired with strong security, could render a solution to securing sensitive data like academic certificates. Before discussing how security can play a role in digital libraries, it is important to first discuss the steps that are involved in digitisation. Planning for digitising a collection is a project that has a beginning and an end.

In a digital library, a project manager is responsible for planning the entire digitisation project. This involves identifying the human resources, financial resources and time frame of the project.

The project manager then allocates tasks based on the size of the project and how many people are available to scan, create metadata, work on a database and website, take responsibility for copyright laws and, once complete, market the digital library. The project manager might devise other responsibilities, since projects vary. Boock (2008) identifies the responsibilities of a project manager as ranging from coordinating the human resources of digitisation within the organisation, securing funding, marketing the final digital library, and approving and prioritising digitisation projects.

Boock (2008) further outlines the different tasks of a digital library, which are enabling search ability of a full-text material by scanning so as to enable optical character recognition in a print item. The proper scanning enables the quality preservation of a digital objects, be it video, or photographs. Another task is the negotiation that has to take place for the material to be digitised; this requires that an investigation be done on who owns the intellectual property rights. Negotiations need to take place with the owner first to ensure that an agreement is entered into before the project starts. The creation of a record when digitising is governed by set standards. It is important to consider selecting one of the metadata structures and schemas (e.g. Dublin Core, MODS, METS), before starting the project of digitisation. In hardware digitisation activities though involving the installation, maintenance, support and customisation of servers and other computer hardware, it is important to factor the sustainability of back-up servers for future. In the selection of digital repository software, it is important to consider carefully whether choosing open source or proprietary software for digital preservation and reformatting.

Figure 2.1 outlines the information flow of a digital library. The diagram illustrates the entire organisation of information for various reasons. The first phase is where the information gets created. This could be achived by various publications which enable creation cycle of a digital library. Each and every record requires identity hence there is generation of meta-data and indexing. The next phase is distribution, at this stage the information is archived, stored and available on network. The seeking phase represents the recommendations made by librarians to the patrons of invormation available which they can use for their research or assignment. This phase also involves patrons doing their own search and harvesting for information that they believe to be relevant. This could be through web interface or face-to-face contact. The utilisation phase represents the patrons having accessed the information they have been searching for. This last phase is where information gets circulated and utilised by different patrons. The time span of the information soon becomes outdated. This leads to an arrow in the diagram which points to the discard phase. When the popularity of material has passed, it sits on the shelves and begins to accumulate dust. There are criteria that are considered when deciding to discard such material. The material could be obsolete or even providing misleading information. When material is discarded, it gets removed from the local library and global holdings.

Finally, distribution represents the long-term preservation of the digitised content associated with the information life cycle (adapted from Borgman 1996).

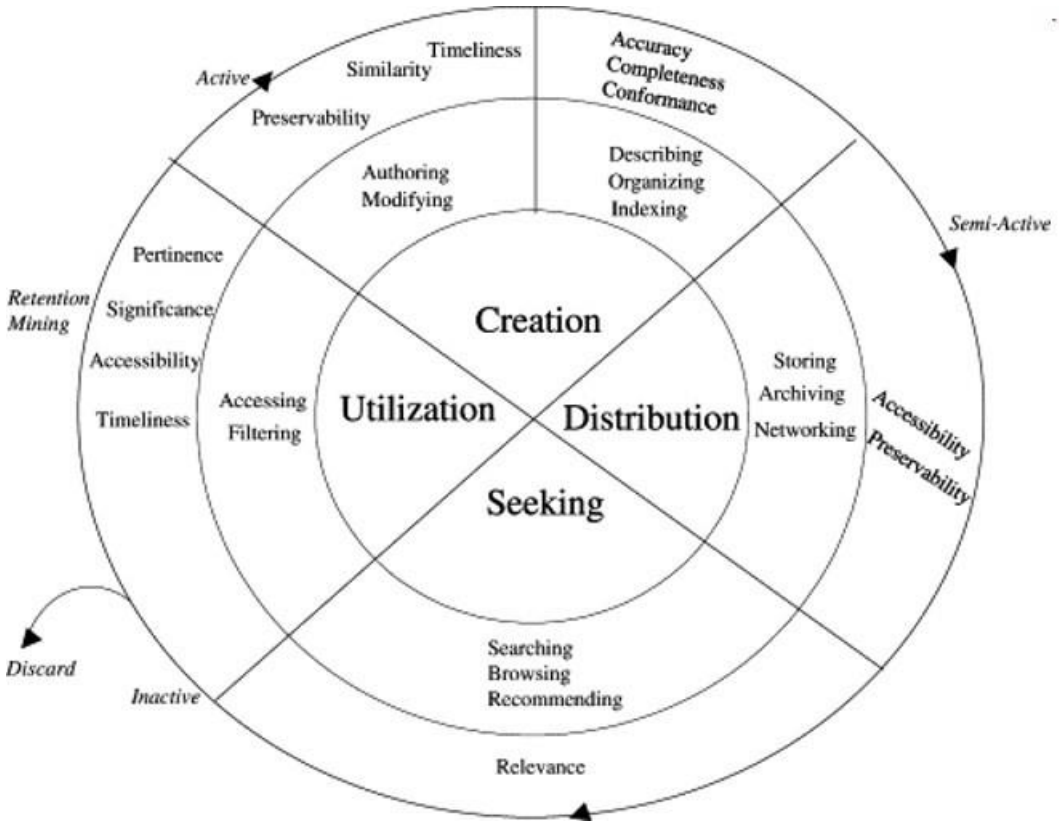


Figure 2.1: Borgman model (Borgman, 1996).

2.7 Types of Digitisation

It is important to support the diagram by further clarifying that there might be many reasons for digitisation. When looking at the different types of digitisation, we commonly observe the types of formatting as well as the access to data and information that is provided by each type of digitisation. Coyle (2006) identifies different types, the first of which is digitisation aimed at preservation. What differentiates digitisation for preservation is that it is used to conserve the freshness and value of the format of the content that is being digitised. The overall aim is to ensure that content can be opened for many years in different machines, including new systems that are yet to be developed. Hence, the content is saved using the tiff format.

Tiff is able to hold large files in their original formats and cannot be opened using a normal browser. In contrast, there is digitisation for discovery. This type of digitisation is focused on discovery of the content; therefore, analogue documents are scanned and optical character recognition performed in order to change the text to a recognised format. This enables the user to be able to discover content using any term that might be on the document.

2.7.1 Digitisation for Delivery

Today's information seekers choose to access information anywhere, anytime, in any format which is different from how it used to be with a traditional library. "Digital files are ideal delivery formats because they can be placed online for user access or emailed. While most digital files are delivered to users over networks, digitisation specifically for delivery often takes the form of an unenhanced facsimile of the original. The text-based digital facsimile is often destined for printing, which includes the provision of digital files by a print-on-demand service. For nontextual media, delivery services like online streaming allow individual users to receive and experience content" (Coyle 2006, 206).

2.7.2 Digitisation for Reading

Though delivery of online print may seem convenient, it is not always a preferred method. There are users whose preferences may not necessarily be to read digitised material but rather to print digitised texts for reading. It should be noted that users digitising for reading may not necessarily be for reading but could be for saving, or storing it for convenience, choice and accessibility, Boock (2008).

2.7.3 Digitisation for Research

Discoverability of data like published papers, in the form of full-text or abstracts, and index is important especially in the Higher Education sector. Therefore, digitisation for research is very important in exposing the already researched and discovered solutions, with availability of references to those who are researching, (Boock 2008).

2.7.4 Digitisation for Machine Manipulation

With the continued discoveries attached to research, digitisation for machine manipulation continues to be important. Data that could be digitised for the purpose could be maps, survey data and satellite data. These data, when digitised, assist in solving problems (Boock 2008).

2.7.5 Born Digital

According to Boock (2008), many organisations have abandoned paying for printers, thereby encouraging their employees to use electronic versions of files only. This has resulted in the

foundation of digital filing and the use of digital formats for all types of work. With this revolution, many new files have recently been created that have never been used in printer form. They are created, utilised and circulated as electronic copies only. Born digital files do present a challenge for long-term preservation, because it is assumed that these files will remain on the system, and if the system should fail, digital files are backed up onto the cloud, thereby allowing for retrieval of these files at any date and from any piece of software or device when needed.

2.7.6 Mass Digitisation

Over the years, companies like Google, JSTOR and Stanford University embarked on the journey of digitising their entire collections. The purpose was to create e-libraries. Mass digitisation, seen as a project of converting all print into electronic copies, came under scrutiny over the copyrights of the individual authors (Coyle, 2006).

2.7.7 Securing Digitised Data

According to Goel and Chen (2008) digitisation has major consequences for security. Companies that digitise have had to invest more monies to ensure that security of data is not compromised.
It seems a proven solution to this challenge does not yet exist.

2.7.8 Evaluation of Digital Libraries

Digital libraries have a human side once they are complete. They allow users to explore how the logic of the process has been put together. Their users must ensure that they get all the benefits from what is perceived to be the original idea of creating them in the first place (Boock, 2008).

2.8 Summary

In summary, digital libraries offer a unique opportunity for libraries and information resource providers to transform their traditional print collections into electronic resources. Though there may be challenges in doing so, the benefits far exceed the downfalls. The integration of security into electronic, digitised materials, could bring a new perspective on the role and functions of libraries. The lack of integration of security in the digitisation process is a gap that this study will focus on, and thus needs to be examined closely. The next chapter focuses on security, particularly the security features used in bank notes, cheques and certificates. The aim will be to

study how steganocryptographic systems can be integrated into digitisation and what their advantages are for sensitive data. The next chapter will focus on the process of securing data by hiding it within other data.

CHAPTER 3

LITERATURE REVIEW: CRYPTOLOGY

3.1 Introduction

Sensitive data is the information that is protected against unneeded disclosure. The reason for protecting information varies from legal, ethical and may as well be for personal privacy. The current way known for securing sensitive data ranges from ensuring that your print or electronic documents are stored in a secured trusted place. Over the years, security techniques such as the encryption systems which uses public key applications, watermarking digital certificates which add signature of source in data, steganography which hide data by embedding it in another data, to name the few have been developed to deal with security breaches as well as to protect confidentiality and integrity of data.

In this chapter, some of the techniques plus the processes which are involved in data security will be discussed. The chapter is structured as follows:

- the first section looks at cryptography,
- the second discusses data hiding,

the third explores watermarking and the final section examines steganography.

While there have been many security software programmes in the higher education industry, the academic literature suggests that there are very few properly researched software programmes that have been adopted by the businesses who conduct risky tasks, like those in the banking system. According to Zheng et.al (2017), while blockchain-based applications are springing up, covering numerous fields including financial services, it is a system that still presents many challenges such as scalability and security problems which still need to be overcome. The literature further suggests that cryptography has been researched and proved to be a highly secure system (Hopper, 2004). Accordingly, a steganocryptographic method is explored as a possible way of securing digital certificates (Blackledge 2008). The following paragraphs discuss the security techniques and methods involved in steganocryptographic systems.

3.2 Cryptography

"Cryptography is the study of mathematical and computational techniques related to aspects of information security" (Blackledge 2008, 1). It is a practice of hiding information that is being sent to another person.

The process involves the practice of changing the information during the process before it is sent to another person and that process is referred to as a code or cipher.

"Cryptanalysis is the art of breaking cryptosystems by using a system for the retrieval of data from encrypted information" (Aktas and Kalkan 2014, 3; and Hopper, 2004). The process is about unlocking the codes and making the information hidden visible; the process is performed by mathematical scripts. In contrast, "Steganography is the study of secret writing which hides data into a form that cannot be interpreted by an observer" (Blackledge and Al-Rawi 2011, 209) and the design of cryptosystems and the estimation of their theoretical security. There are various methods used for "the design of security software, which should ideally be safety-critical" (Gebotys 2004, 1). "Cryptography is the best solution against the unauthorized use of the information" (Rincu and Serbanescu 2009, 113).

The introduction of attacks to the cryptosystem are a safe way of testing the strength of the system. However, it should be noted that with an increase of sophistication in technology any new unknown attacks may be introduced today. "The practical realities associated with cryptology are indicative of the fact that security is a process and not a product" (Blackledge and Dubovitskiy 2011, 20). According to Hopper, when discussing the origin of information hiding, "Shannon started cryptography and introduced the concept of securing information" (Hopper 2004, 02). Shannon's idea was to hide information behind other information. The security of information would be between the person sending information and the person who is receiving the information. The system was designed to hide information from those who are not intended to know about it. Further developments allowed the researchers an opportunity to work on a theory of Security. "The system was designed to allow people who are aware of the information to have generated pins for unlocking the information" (Hopper 2004, 03; Goldwasser and Micali, 1982).

3.3 Information or Data hiding

Blackledge and Al-Wari (2011) defines in detail the process of hiding data as follows: "…A digital image can be used to hide messages in other images" (Blackledge and Al-Wari 2011, 2).

A detailed description of how this process works is explained as follows: “A colour image has 8 bits to represent the red, green and blue components. Each colour component is composed of 256 colour values and the modification of some of these values in order to hide other data is undetectable by the human eye.

This modification is often undertaken bychanging the least significant bit in the binary representation of a colour or grey level value. For example, the grey level value 128 has the binary representation 10000000.

If we change the least significant bit to give 10000001 (which corresponds to a grey level value of 129) then the difference in the output image will not be discernible. Hence, the least significant bit can be used to encode information other than pixel intensity. Further, if this is done for each colour component then a letter of ASCII text can be represented for every three pixels. The larger the host image compared with the hidden message, the more difficult it is to detect the message” (Blackledge and Al-Wari 2011, 58). There are two methods that can be used to hide information, watermarking and steganography, which will be discussed in the following sections (Su, 2003; Che-Wei and Wen-Hsiang, 2012).

3.4 Watermarking

“Watermarking is the practice of hiding a message about an image, audio clip, video clip, or other work of media within that work itself” (Cox 2007, XV); the process is done in such a way that the quality does not get degraded. The embedding is permanent and can be detected whenever needed. “The information hidden by a watermarking system is dealing with the object to be protected” (Shad 2011, 2). While watermarking has proven to withstand security weaknesses in print documents, there are some challenges, such as sensitive data being visible in the eyes of the intruders which allows intruders an opportunity create a sophisticated system for tampering with the data. Due to the limitations of watermarking, the focus of this study is on steganography, which is discussed in the following paragraph (Shad, 2011; Hopper, 2004; Hallot, 2008).

3.5 Steganography

“Steganography is the study of the techniques used to hide one message inside another, without disclosing the existence of the hidden message or making it apparent to an observer that this message contains a hidden message” (Blackledge and Al-Wari 2001). The purpose of steganography is to bypass the intruder and ensure that the message and communication is

happening between two parties; if the message and communication are detected it could result in a successful attack on this system. (Hopper, 2004; Zawilska, 2012).

Blackledge and Coyle (2010) define steganography as "the only method that hides data behind data in such a way that it is the intended recipient who knows about the existence of message. The message does not attract attention from an unintended messenger" (Blackledge and Coyle 2010, 56). Steganography is the only system that has the capacity to securely hide data behind data and that allows easy retrieval of the hidden data. The reason for hiding data is to make files less attractive to hackers, who might miss an opportunity to detect high-value information. However, there is a need to understand why steganography might be a better method for securing data than other software that has been in existence for many years (Aktas, 2014).

While many security software programmes have been developed, tested and utilised in the market, problems have been presented by many of these methods of fraud prevention, like the digital signature. Chen-Wilson, Gravell and Argles (2011) claim that forged certificates using the digital signature method are caused by poor security in e-portfolio systems, as the challenge with a digital signature is that while the signer and the issuer can be validated, the content of the document cannot. One of many weaknesses of the digital signature is that potential hackers know the system is meant to prevent fraudulent activities, like the forgery of another person's identity.

Many authors seem to have identified steganocryptographic technology as the method that offers the most relief from the risk of being targeted for fraud or hacking. Atawneh et al. (2013) state that adaptive steganography has the ability to embed the secret information in a specific location on the cover of the image, making it more secure. Cheong et al. (2013) claim that the use of smartphones has opened up business opportunities, such as electronic ticket payment; however, security remains the top priority for consumers. Therefore, the integration of steganographic passwords offers customers an opportunity to customize their own access control. Satir and Isik (2012) discuss the advantages of using steganography in text emails by emphasizing that the application of steganography does not cause any constraints on emails, and that the method is not language-specific, meaning that it can be applied to text in any language.

The steganocryptographic method has the capability to transport sensitive data online with little chance of data falling victim to hackers. Blackledge and Coyle (2010) outline the encryption and decryption processes, involving input, output, operations and pin-generated login. The software has the advantage of being applicable in different formats while still embedding the data in the same way, which is an advantage for users of different formats. Rafat and Sher (2013) discuss the use of steganography in ASCII files.

There are studies which suggest that the steganocryptographic software has been applied and delivered excellent results in securing sensitive data. Agrawal and Savvides (2009) have tried a different form of embedding biometric data in coefficients of cover images, which can be exploited for hiding any type of image, fingerprint or iris code. The results were excellent, indicating that steganography is one of the best methods of authentication. Notwithstanding these and many other authors who have presented the application of steganography in many different areas, there are researchers who have identified disadvantages of using steganography. For example, Adesina et al. (2011, 2) compare "a number of different security methods" and look at the drawbacks of using steganography in the communications of health care systems.

Finally, the literature focuses more on the advantages of using software in electronic transmission of sensitive data and says little about the application of the software to the preservation of sensitive data, which is a gap that needs to be explored further. It is for these reasons that this study will focus on demonstrating and illustrating the software for the preservation and securing of degree certificates at UKZN. This allows the study to explore the question of whether digital preservation together with security can be utilised to archive and secure sensitive data. Furthermore, it will help to explore what digital preservation entails and how it has been utilised over the years.

3.6 Summary

Watermarks hide work within itself, while steganography hides work in another work. The literature reveals that extensive research has been done on the different kinds of tools with which steganography has been used successfully. However, there is no literature that reveals how steganography has been used in libraries to secure, archive and preserve sensitive data. The next chapter reviews the underlying theories in information systems security management research practice, in order to guide this study.

CHAPTER 4

LITERATURE REVIEW: NATURE OF THEORY IN INFORMATION SYSTEMS

4.1 Introduction

This chapter explores the theories used in information systems. The previous chapters reviewed the security of documents in general and further looked at particular methods utilized in securing sensitive data. Therefore, the combination of digitization and security will be explored by the study. It is important to now locate the value-add of the study in information systems theories. This is achieved by reviewing the theories commonly used in information systems and identifying those most relevant to this study.

4.2 General theories

Kerlinger and Blalock (1986), Whetten (1989) and Bacharach (1989) identify the following characteristics for a theory in general:

- It should have an identification of constructs;
- The relationships of identified constructs are clearly specified, and
- Those relationships are falsifiable.

"Research without any underlying theoretical reasoning is meaningless information" (Mills 1959, 3), while "theory without research is abstract and speculative" (Newman 1999, 8). These arguments present the inter-relationship of theory and research. Therefore, for research to be effective, a researcher needs to understand the role of theoretical argument or reasoning in the research process. It is then presented as a scholarly writing with the aim of presenting the original ideas and convincing the audience that those ideas are valid by presenting an organized argument. It is thus clear that theoretical reasoning is an argument which is an interactive and goal-directed facility for the creation of scientific knowledge. The modes of theoretical reasoning are retroduction, abduction and induction which is defined as "inferences from observed to unobserved things" (Price, 2005, 93) and is classified under critical realism and positivism; induction is defined as the "inference from past to future" (Price 2005, 93) and is classified under interpretivism research. The next section looks closely at the theoretical arguments which are used in information systems.

4.3 Information systems theory

Gregor (2006) reviews the answers from various authors in the information systems (IS) field to questions about theories in IS, around domain, epistemology, socio-political perspective, as well as structural nature and form.

The question "about the domain of interest of IS remains a topic of interest since the founding of the discipline" (Gregor 2006, 2). The debate is on distinguishing the IS discipline from other disciplines and finding its unique nature. Epistemological questions have received attention from various authors who question the merit of different paradigms for conducting research in IS while distinctions between positivist and interpretivist, and between qualitative and quantitative methods, are being debated. Mingers (2001) argues for pluralism in methods, and Lee (1991) favours integrating approaches. Benhasat and Weber (1996, 2) and Robey (1996, 2) interpret the issues "of political, power and prestige in relation to the discipline as part of the benefits and costs of diversity in IS research". This focused on the question of relevance to the practice of IS. Kuhn's (1996, 3) analysis examines "how the interpretivist paradigm has emerged historically in constrast to positivism". Ngwenyama and Lee (1997) look at the improvement of human conditions in IS research by focusing on addressing ethical and moral questions. "Many IS researchers who use the word 'theory' in their work fail to give any explicit definition of their own view of theory" (Gregor 2006, 612).

According to Livari (1993), Markus et al. (2002) and Walls et al. (1992), the different types of theory should be used in the explanation of how the theory structure for a specific study is constructed. Authors in the IS field define theory as follows:-

- "As statements that indicate how something should be done in practice" (Davis and Olson 1985 in Gregor 2006, 613). According to Davis and Olson (1985) in (Gregor 2006, 613), "a theory in IS communicates the way in which Management Information System should be designed, implemented and managed". Cushing (1990) added that "this theory provides prescriptions to be followed in practice" Cushing (1990) in (Gregor 2006, 613), "with the implicit expectation that the prescribed methods will be better than alternatives".
- "As providing a lens for viewing or explaining the world (Orlikowski and Robey 1991, 613)" in (Gregor 2006, 613) saw a theory where "the organizational consequences of information technology are the products of material and social dimensions" which make it the end product.

- "As statements of relationships among constructs that can be tested" (Davis 1986 in Gregor 2006, 613) introduced the "technology acceptance model which is based on" two particular beliefs: that of user "perceived usefulness and perceived ease-of-use, which are of relevance for computer acceptance behaviour" (Davis 1986 in Gregor 2006, 613). "This theory leads to testable propositions which can be investigated empirically" (Rosemann and Vessey 2008, 4), which points out what is found in previous studies which suggest that in the information systems discipline, there is a lack of sufficient relevance to practice; they suggest a need for the intervention effect which is geared at "achieving practical relevance and acceptability of research in practice" (Rosemann and Vessey 2008, 5).

Information systems security (ISS) management is one of the areas which shows a huge gap between theories used and practical intervention This is witnessed by daily reports of information systems security and privacy breaches (Siponen and Baskerville, 2018). The ISS problem is big and continue to cost companies millions daily.

4.4 Nature of Theory in IS

According to Gregor (2006), there are different types of research in IS. There are theories "for analysing for explaining, for prediction, for explanation and prediction, and for design and action" (Gregor 2006, 6). These different types of theories are discussed in detail next.

4.4.1 Theory for Analysing

"The theory for analysing analyses what is and does not explain the cause nor make any generalisations" (Gregor 2006; 624). It is a theory that focuses on the characteristics of the study which is in context. The study could be about events or people. According to Fawcett and Downs (1986,) the theory of analysing is very critical in a study where there is no knowledge about the context or subject. The advantage of this theory is that it then provides the description and further looks at relationships present in that particular study. Alternatives to this theory type are classification schema, framework and taxonomies. The contribution to knowledge with this theory is that when little is known about something, information gathered brings credibility to what is (Miles and Huberman, 1994).

4.4.2 Theory for Explaining

"The theory for explaining focuses on how and why some incident happened" (Gregor 2006; 624). This theory focuses on helping with the view and understanding of the world in order to explain why things happen the way they do. According to Klein and Myers (1999), this theory can be seen as a sensitising tool to view the world, while DiMaggio (1995) see it as a tool that enlightens us about the world.

One of the theories that illustrate this is from Giddens (1984). This type of theory includes structuration, which is "an understanding of the world as reciprocal relationships between action and social structures" (Giddens 1984, 16). Latour (1991) refers to this theory as an actor-network theory, which means that it is "an understanding of inanimate objects and material systems as actors" (Latour 1991, 4). If this theory is to be related to information systems, it could be observed in case studies of failures in IS, which Avison et al. (2006) refer to as sometimes caused by "a lack of managerial attention to recognise IT governance" (Avison et al. 2006, 10).

According to Gregor (2006), the contribution to knowledge through this theory is that it explains something that was poorly or imperfectly understood. "Judgement regarding the contribution to knowledge for this type of theory is made primarily on the basis of whether new or interesting insights are provided, and also on the basis of plausibility, credibility, consistency, and transferability of the arguments made" (Gregor 2006, 625).

4.4.3 Theory for Prediction

"This type of theory focuses on the future of what the study in context will be. It does not explain why it will be. This type of theory is not commonly used in the IS field" (Gregor 2006, 625). This theory is more commonly used in econometric studies and finance. The contribution to knowledge through this theory is to do with "discovery of regularities that allow prediction which can be of interest, if these were unknown before" (Gregor 2006, 625), and also its practical importance.

4.4.4 Theory for Explanation and Prediction

"This type of theory for explaining and predicting (EP theory) mentions what is, how, why, when and what will be. EP theory implies both the understanding of underlying causes and prediction, as well as description of theoretical constructs and the relationships among them" (Gregor 2006, 626).

This theory includes a number of theories, including general systems theory and related information theory. It is a theory that is modelled in terms of input, throughput, output, feedback, boundary and environment. The "Technology Acceptance Model by Davis et al. (1989) is one examples of this theory" (Davis et al. 1989, 6). The contribution to knowledge through this theory could be through theory building or theory testing. The study is informed by the Unified Theory of Acceptance and Use of Technology as a framework and seeks to explore whether the intention to use the system has a relationship to performance expectancy, effort expectancy, social influence and facilitating conditions. The contribution of the theory will be testing the consistency in UTAUT which provides agreement with the evidence. Therefore, this theory is appropriate for this study.

4.4.5 Theory of Design and Action

The theory of design and action focuses on doing. "It is about the principles of form, function, methods and justificatory theoretical knowledge that are used in the development of IS" (Gregor 2002, 628).

Various authors regard this theory from different though complementary perspectives. Morrison and George (1995) refer to this theory as playing a part in software engineering research. Burstein and Gregor (1999) regard this theory as critical in systems development. Hevner et al. (2004) refer to this theory as a design science. "A framework to demonstrate the relationship activities of design and natural science research was developed which identified four products of design science being constructs, models, methods and implementation" (March and Smith 1995, 4). Hevner et al. (2004) expanded their ideas by putting emphasis on the artifact as the contribution of design science.

The contribution to knowledge is "utility to the community of users, novelty of artefacts and the persuasiveness of claims that are effective" Hevner et al. (2004, 5). Further to this, "models and methods can be evaluated for completeness, simplicity, consistency, ease of use, and quality of results obtained through use of method" (Hevner et al. 2004, 5).

This study will be drawing on EP theory as it examines the knowledge and perceptions of people and information technology capabilities. It will indirectly draw on some of these theories. Future studies could investigate the impacts these artefacts have in the workplace and in society.

4.5 Current practice of Information Systems Security Management

Since information systems security (ISS) research originates from a problem, it means the major role it plays is to contribute a solution to an existing practical problem. Therefore, "philosophically, a practical motivation which is a problem in practice is the key epistemic goal of ISS research, rather than seeking truth or new knowledge" (Siponen and Baskerville 2018, 248).

In the current "ISS research, the theories, models or hypotheses are not compared with best practices or closest competitors" (Siponen and Baskerville 2018, 250). It is not asking "how can I show that my findings can outperform current best practices in solving the problem? rather, ISS research can show that a theory-based hypothesis meets some crucial test" (Siponen and Baskerville 2018, 250).

An introduction of information technology (IT) artefacts and theory contextualization in ISS research was made by Hong et al. (2014). However, there is urgent need "to show that an IT artefact or contextualization of theory solves the problem well than practical solutions" (Siponen and Baskerville 2018, 250). Rather, this was a shift from "emphasis on problems and solutions, to showing that the theory-based explanations are true or empirically supported" (Siponen and Baskerville 2018, 259). There is no emphasis on application effectiveness or comparison with best practices.

The results of the current ISS research in practice is that "it does not indicate the best approach to practitioners or highlight which of these empirically tested theories are the most effective for solving the ISS problems" (Siponen and Baskerville 2018, 259). This could result in practitioners turning to an experienced-based report when seeking to improve their information security management. The gap that remains in the ISS research field is a practical problem solver driven research.

4.6 Summary

This chapter reviewed relevant information systems theories and their contribution to the body of knowledge. The theory for explaining and prediction has been chosen because it contributes to the process which looks at the unfolding of events over time. This study aims to address the gap in the ISS research of problemsolving effectiveness. Therefore, this study focuses on trying to find a solution to a practical problem which will serve as a contribution of the study. A

model/theory can be developed or extended using the relevance in a combined problem-solving solution, driven by theory. The next chapter discusses the chosen methods, framework and methodologies of this study.

CHAPTER 5

RESEARCH METHODOLOGY

5.1 Introduction

This chapter gives a discussion of the research paradigms, methods and philosophies preferred for the study. The author discusses and support an argument in defence of the approaches used in this research, as well as the argument against those that were not employed here. A detailed outline of the research strategy is presented to illustrate the progression of the research in answering the questions and objectives that were set in Chapter 1. In summary, this chapter will describe the philosophical stance believed by the author to be the best suited to answer the research questions. Other paradigms will be discussed that may influence the results of the study. The philosophical approach underlying this study is the theory for explaining and prediction while drawing from interpretivism and positivism using mixed methods. The reason for choosing this approach is because EP theory focuses on "understanding of underlying causes and prediction, as well as description of theoretical constructs and relationships among them" (Gregor 2006, 618). This relates well to what the interpretivist does, which is the understanding of the context of the world from individual experiences. In this study, it is how the context influences information systems and how it is influenced. Positivism states that every rationally justifiable claim can be proven. This study attempts to find what works in securing and archiving sensitive documents. The mixed methods approach is chosen because it brings the collaborative approach to the research. Therefore, it will be important for the study to apply qualitative and quantitative analyses in order to find the best answers to the research questions.

5.2 Research Paradigms

The word 'paradigm' means worldview, and originates from the Greek word paradeigma, which means what is acceptable in society (Kuhn 1977). In research, 'paradigm' means a reasonable system shared by a group of researchers that provides a helpful model for analysing issues and finding an answer (Kuhn 1977; Olsen, Lodwick and Dunlop, 1992). The relationship of paradigm, standards and ideal models is that paradigm represents the worldview, by which exploratory standards exist to form an understanding via models which are merely human constructs. As indicated by Guba and Lincoln (1994), "exploratory standards" are convictions that guide human activity, while Saunders et al. (2007) characterize ideal models as those

models that specialists propose with the aim of increasing comprehension and concentration under scrutiny. Hence, examining the researcher's worldview is imperative, since it impacts the results of the research conducted. There are three segments of standards, specifically: methodology, epistemology and ontology (in Denzin and Lincoln, 2005).

5.2.1 Methodology

Methodology deals with the procedures by which information is efficiently gained in a specific research endeavour to solve the existing problem or prove the hypothesis. The use of methodology allows for the construction of approaches to inquiries, which are methods to discover new knowledge. Methodology is the overall group of methods used to gain meaning about the world (Denzin and Lincoln, 2005).

5.2.2 Epistemology

Epistemology is the examination of what differentiate guarded belief from assumption. "It manages the hypothesis of information particularly about its strategies, legitimacy and extent of the review. Epistemology addresses some of the following inquiries: What is learning? What constitutes worthy information in a field of study? What is the relationship between the inquirer and the known? (Guba and Lincoln 1994, 106)." Epistemology provides evaluative criteria for information claims and endeavours to identify what separates demonstrated learning from other learning structures; consequently, it creates new meaning about various learning claims (Krauss, 2005).

5.2.3 Ontology

Ontology deals with existence and actuality. It deliberates about what exists and what is genuine. Metaphysics as a philosophy is concerned with reality as well as nature. The two arms of metaphysics "are objectivism and subjectivism (Saunders, Lewis and Thornhill 2007, 7)." "Objectivism is the view that there are social elements external to social players who are anxious abouttheir reality (Saunders, Lewis and Thornhill 2007, 7)." Subjectivism is the view that a social marvel is made from observations, and the resulting activities of those actors concerned with their reality (Saunders, Lewis and Thornhill 2007).

5.3 Classification of Research Paradigms

Gregor (2006) examines the "structural nature of theory in the discipline of information systems and proposes a taxonomy that classifies information systems theories according to the manner in which four central goals are addressed, that is, prescription, explanation, analysis and prediction (Gregor 2006, 614)." From these taxonomies, five inter-related "types of theory are distinguished, which are the theory for analysing, theory for predicting, theory for explaining, theory for explanation and prediction and theory for design and action" (Gregor 2006, 615). It should be noted that that there are common theory terms used amongst these and that only four paradigms are discussed in this research.

The four traditional paradigms, pragmatism, realism, interpretivism and positivism, will be discussed in detail.

5.3.1 Realism

'Realism' deals with scientific enquiry into knowledge (Saunders, Lewis and Thornhill 2007, 3).
Its philosophy is of theoretical perceptions which are detached from the knowledge of existence.

"There are two major forms of realism" (Bryman 2004, 12). Empirical realism states that the best way of understanding the reality comes from theutilization of suitable methods. Critical realism "recognizes the reality of the natural order and events and discourses of the social world" (Bryman 2004, 12). The idea is human beings need to understand the world and be able to change it from this perspective.

5.3.2 Interpretivism

The 'interpretivist' paradigm stresses the need to put analysis in context from the perspective ofunderstanding the world and how "it functions which is done from the subjective experiences of people" Reeves and Hedberg (2003, 32). It uses meaning, such as interviewing, which is a subject relationship between the researcher and subject. "Interpretive approaches give the researcher greater scope to address issues of influence and impact, for example by asking questions, such as why and how particular technological trajectories are created" (Deetz 1996, 28). This type of theory focus on human interaction with the world. "The purpose of the interpretive approach in information systems is to produce an understanding of the context and the process whereby information systems influence and are influenced by the context" (Walsham 1993, 6). According to Kaplan and Maxwell (1994, 12), interpretive approaches

focus on the “full complexity of human sense-making as the situation emerges”. They aim to find meaning from the social interactions of the people with the objects in the world. “The interest of interpretivists is not the generation of a new theory, but to judge, evaluate and refine”. (Bryman 2004, 13). Therefore, both pragmatism and interpretivism address essential features of shared meaning and understanding. Pragmatism differs in that it extends the meaning. “There are three different uses of theory in interpretive case studies: theory guiding the design and collection of data; theory as an interactive process of data collection and analysis, and theory as the outcome of a case study” Walsham (1995, 31).

It is ideal for a researcher to have a full grasp of what they are researching and apply relevant theories suited before the collection of data is implemented. “An interpretive study seeks out meanings held by the researcher and actors within the case, although it is difficult for the researcher to be completely detached from the object of study” (Miles and Huberman, 1994, 8). The study is conducted in an environment which the researcher is familiar with.

5.3.3 Positivism

‘Positivism’ states that “every rationally justifiable claim can be scientifically verified or proven”. (Bryman 2004, 11). Myers (1997) emphasizes that positivists make the assumption that reality is objective. This epistemological declaration claims that “verifiable research should be conducted in a controlled environment, where observable social reality is measured using structured methodology” This type of research is ideal for a study that is conducting a test to address hypothesis. (Bryman 2004, 11). “Positivistic research converges on the true state of events. Positivism is widely held among natural scientists who attribute the success of current scientific breakthroughs in a modern world searching for answers” (Hussey and Hussey 1997, 4) and (Capra, 2002). The study conducted will not use the positivism theory approach as it not relevant.

5.3.4 Pragmatism

Pragmatism is about action and change. In terms of knowledge, it is regarded as the development of constructive knowledge. Pragmatism collects data through assessment and intervention, and the researcher is engaged in change. It facilitates change as a solution. The central function of pragmatism is to intervene in the world and provide a solution rather than simply observe the reality (Creswell 2007, 2). Interpretive information systems research deals

with the world, where actions and interactions are facilitated by humans through inter-relationships and interactions (Creswell 2007, 5). “Pragmatism is not committed to any one system of philosophy and reality, as it allows researchers to draw liberally from both qualitative and quantitative methods to address the research question” (Goldkuhl 2012, 9). Individual choice of methods to be utilised is depended on the type of study to be conducted. Pragmatism is concerned with change that is about intervening in the world. “Pragmatism addresses essential features of shared meaning and understanding, and thereby extends meaning” (Goldkuhl 2012, 7).

5.4 Research Framework for the Study

TerreBlanche and Durrheim (1999) emphasize that the research process must employ a combination of ontology and epistemology, which relate to how people view the world and methodology. This may involve one or more paradigms, depending on the kind of research; therefore, the IS theory, Unified Theory of Acceptance and Use of Technology (UTAUT) while drawing on interpretivist and positivist paradigms will be utilised for this research. “Information technology acceptance and use has a long and rich tradition in the information systems literature, and it remains a major stream of research in the information systems field” (Gregor 2006, 613). Since the initial work of Davis (1989), there have been a number of developments, with new theoretical models adding to Davis’s model and further explaining technology acceptance and use, (Ajzen and Fishbein, 1985), Ajzen and Fishbein, 1980), (Venkatesh and Davis, 2000) and (Venkatesh et al., 2003).

“Rooted in Ajzen and Fishbein’s model, the Theory of Reasoned Action (TRA), introduced and developed the technology acceptance model (TAM) to provide a theoretical explanation of the relationship of attitude-intention-behaviour” (Davis et al. 1989, 2). The theory focused on the relationship between computers and human beings. “TAM received empirical support for being strong and parsimonious in forecasting technology acceptance and adoption”. (Venkatesh et al. 2003, 13). It illuminated the fact that there is going to be a relationship between someone’s behaviour, intention and the performance of the task. In this model, “two specific variables, perceived usefulness and perceived ease of use, were hypothesized to be the fundamental determinants of user acceptance” (Venkatesh and Davis 2000, 4).

5.4.1 Perceived Usefulness and Ease of Use

“Perceived usefulness is defined as the extent to which a person believes that using a particular technology will enhance his or her job performance”, (Davis et al. 1989, 8) and “this variable

has a direct impact on people's intention to use technology". According to Davis et al. (1989, 9), "perceived ease of use is the extent where someone using the system will be free of effort. It is possible that people who believe a technology to be useful could, at the same time, believe it to be too difficult to use, such that the performance benefits of usage are outweighed by the effort necessary to use it" (Davis et al. 1989, 11). Many studies provide evidence of the impact of perceived ease of use on attitudes towards usage and behavioural intention (Sumak et al., 2011).

"Perceived ease of use is a significant determinant of people's attitudes and intentions to use technology and has been noted in technology acceptance research that perceived ease of use affects behavioural intention both directly and indirectly, via attitude" Wong and Teo (2009, 8).

5.4.2 Attitude towards Computer Use

"There is a growing body of research that suggests that attitudes towards computer use have a strong link to behavioural intention" and, thereby, to actual behaviour (Davis 1989, 9), (Wong and Teo, 2009) and (Sumak et al., 2011). "Behavioural intention is used as the dependent variable in this study as it is known to be a more practical way to measure technology use" among UKZN employees (Teo and Noyes 2011, 6). As such, "it is deemed more accurate to measure an employee's intention to use a computer than to measure their actual usage" (Wong and Teo 2009, 6). The way people respond to technology is related to their attitude on the utilisation of cimputers. "Interest in the study of technology acceptance has grown since the publication of Davis's technology acceptance model" (Venkatesh et al. 2003, 16) and has led to the development of as many as eight main competing models for predicting technology adoption, acceptance and usage.

"To bring more meaning to the technology acceptance literature and to provide a unified view of this field", (Venkatesh et al. 2003, 7) developed UTAUT, which identifies four predictors of information technology acceptance and usage:" "performance expectancy, effort expectancy, social influence and facilitating conditions. Gender, age, experience and voluntariness of use are moderators of the relationship between these predictors and technology usage intention and use behaviour" (Venkatesh et al. 2003, 8).

The figure depicts the links from performance expectancy, effort expectancy, social influence and facilitating conditions to behavioural intention and user behaviour, with experience, voluntariness, age and gender as moderating factors.

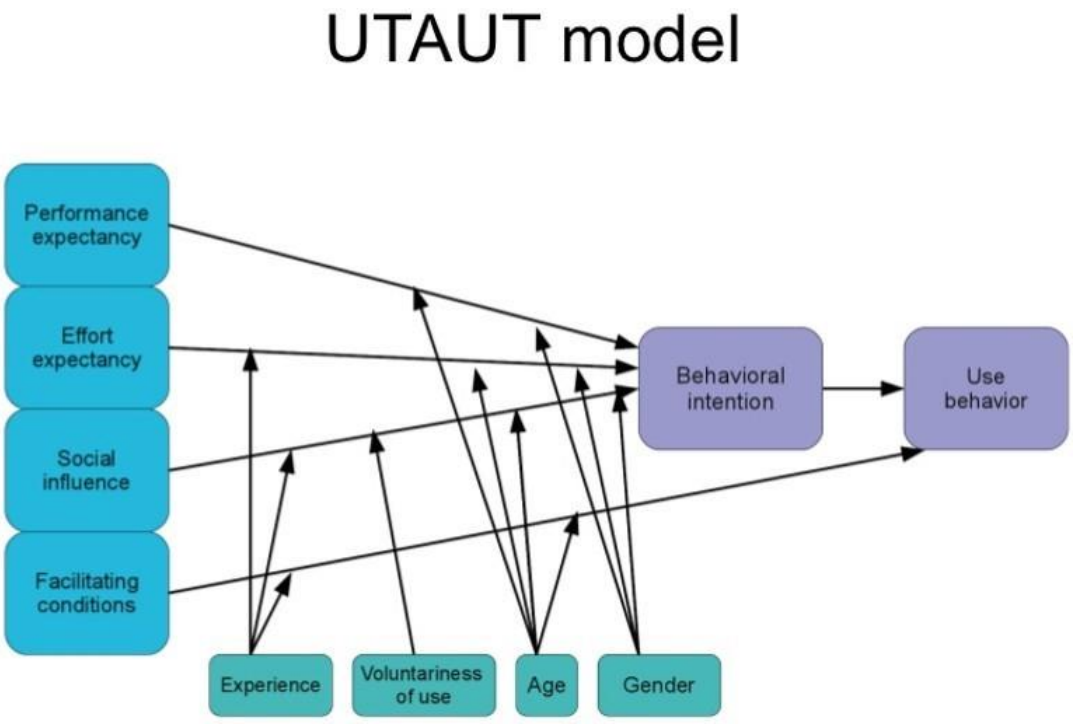


Figure 5.1: Illustration of UTAUT model (Alzubaidi, 2011).

5.5 Research Approach

"There are three types of practices in research, namely, qualitative, quantitative and mixed methods" (Mertens 2005, 5). Qualitative research is the investigation of the meaning that social actors attribute to an occurrence and the creation of an understanding of events (Ragin, 1992), (McNabb, 2004). Quantitative research, on the other hand, has the ability to analyse and challenge theories by looking at the relationships amongst variables. This is mainly done to simplify and reproduce research conclusions in a controlled environment. A mixed-method approach combines both qualitative and quantitative approaches. It uses the force of "both methods in an inquiry, researchers who hope to avoid the bias and limitations of any one strategy of inquiry opt for this method, as this study does" (Creswell, 2007, 8).

Johnson and Onwuegbuzie (2004) recommend mixed methods be used when the research question suggests that combining quantitative and qualitative approaches will help with distinct research outcomes.

"Using mixed-method techniques results in the collection of richer data, thereby leading to a greater understanding of the underlying phenomena" (Johnson and Onwuegbuzie 2004, 4). These researchers note that by combining both qualitative and quantitative methods, the study will offer flexible investigative techniques.

5.5.1 The reason for using mixed methods

By combining qualitative and quantitative findings, "an overall or negotiated account of the findings can be forged, not possible by using a singular approach" (Bryman, 2007 in Ostlund et al., 2011, 370). This puts a study which is done using a mixed method approach at an advantage. "The growing need for cost effective research and the shift in focus from theoretically driven research to research which meets policymakers and practitioners' needs and the growing competition for research funding" (Brannen, 2009 in Ostlund et al., 2011, 370) makes mixed methods research relevant. The advantages of a mixed study could be traced on the quality of data and on the addressing the daily issues related to the problem statement. "Mixed methods can also help to highlight the similarities and differences between particular aspects of a phenomenon" (Bernardi et al., 2007 in Ostlund et al., 2011, 370). This is another advantage where a study that has used both methods could have quantitative and qualitative results supplementing each other.

5.5.2 Characteristics of mixed methods

"The characteristics of mixed methods studies involve integration of the qualitative and quantitative findings at some stage of the research process, be that during data collection, analysis or the interpretative stage of the research" (Kroll and Neri, 2009 in Ostlund et al. 2011, 370).

There are various approaches that could be used. There is concurrent data, parallel data and sequential data analysis. The difference between these approaches is that a concurrent approach utilises both qualitative and quantitative data sets simultaneously. Parallel data analysis is where data collection is done separately.

A third approach is "sequential data analysis, in which data are analysed in a particular sequence with the purpose of informing rather than being integrated with the use of or findings from the other methods" (Onwuegbuzie and Teddlie, 2003 in Ostlund et al., 2011, 379). This approach may help in instances where the qualitative and quantitative data yielded completely different results. It could be that the results are reported with no intention of establishing the link between quantitative and qualitative data.

Figure 8.1 illustrates the "points of the triangle which represent theoretical propositions and empirical findings from qualitative and quantitative data, while the sides of the triangle represent the logical relationships between these propositions and findings. The nature and use of the triangle depends upon the outcome from the analysis, whether that be convergent where quantitative and qualitative findings lead to the same conclusion, complementary, where qualitative and quantitative results can be used to supplement each other or divergent, where the combination of qualitative and quantitative" (Ostlund et al., 2011, 388) results provide different findings. This figure highlights the advantages of utilizing the qualitative and quantitative approach whereby both empirical and theoretical findings could be established in a study. Results from qualitative and quantitative data could generate agreement or differences.

"Each of these outcomes requires a different way of using the triangulation metaphor to link theoretical propositions to empirical findings" (Erzberger and Kelle, 2003 in Ostlund et al., 2011, 380). This is where the richness of combining both qualitative and quantitative methods could be analysed and outlined in detailed. Figure 5.2 below illustrates the use of triangulation of the UKZN respondents on the user acceptance of the systems.

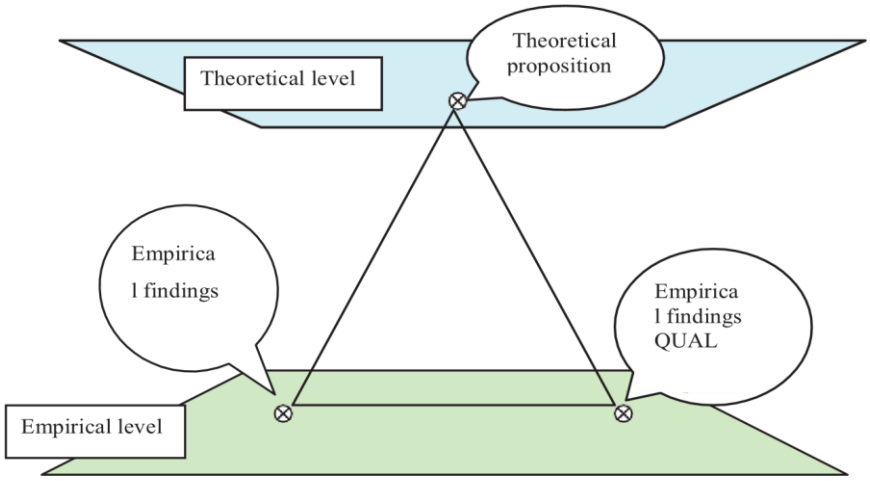


Figure 5.2 "Illustrating the triangulation triangle" (Erzberger and Kelle, 2003 in Ostlund et al. 2011, 381).

"Triangulation is done to examine the validity of both quantitative and qualitative research results. Triangulation is with the aim to better understand through complementary findings a result that could also exist on its own, or to place it in a broader context. Triangulation is a way of generating a complete result with the help of two partial findings that could not stand on their own" (Kelle et.al., 2019, p11).

"Comparing the results from multiple methods aimed to minimize the chance that the weaknesses of any single method might produce invalid conclusions" (Morgan, 2019, p6).

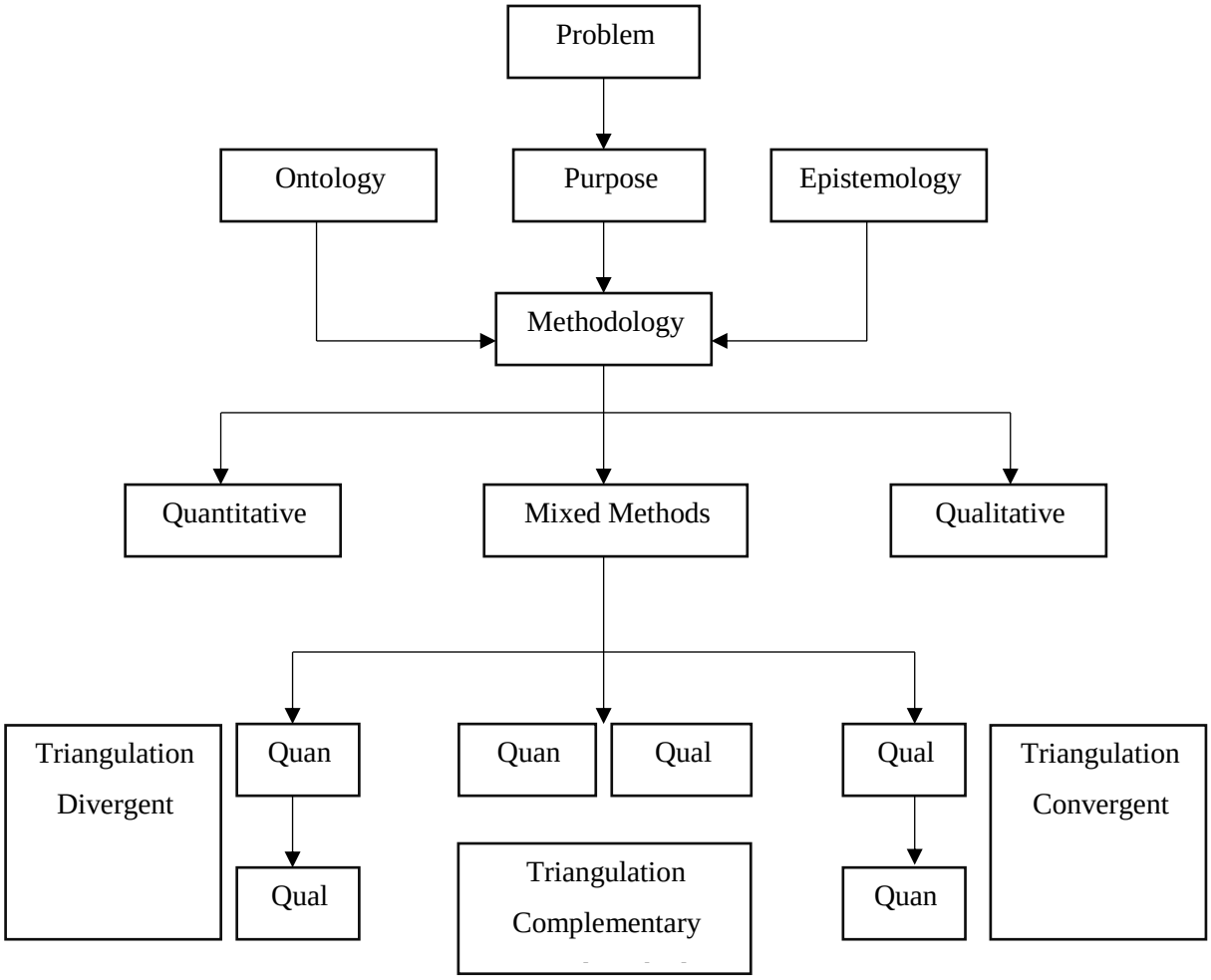


Figure 5.3 Paradigm and methodology map

The above figure shows a sequence of the how the research questions will be answered using a mixed method approach. The triangulation approach will be used for research questions one and four:-

1). To what extent do various factors influence user acceptance of information security systems methods for securing and archiving information at UKZN?

4). To what extent does the current system used to archive academic certificates at UKZN display problems related to employee perceptions of the university's information systems security measures?

The first analysis of mixed methods is used to establish how qualitative and quantitative results supplement each other.

The second analysis of the exploratory sequential mixed method will be used to answer question one and question four of the study. The results of these questions will be analysed to establish convergent triangulation in the results.

The third analysis of explanatory sequential mixed method will be used to answer question one and question four of the study. The results of these questions will be analysed to establish the triangulation of divergent in the results.

The triangulation to develop a theory that will use all four questions and the rest of the questions which are as follows:

2). To what extent do University of KwaZulu-Natal employee perceptions regarding the information systems security measures at UKZN, affect their intention to use these measures?

3). To what extent do others' beliefs about the use of information systems security measures affect UKZN employee perceptions of and intentions to use these measures?

5.6 Research Design

The design of a research study is occasionally influenced by random occurrences or the researcher's own views. The research theory, framework and methods selected guide how the research problem is examined and which tools are used (Creswell, 2007). Selecting the relevant tools to investigate the problem is ideal for research outcome (Morse, 1994). Table 4.1 is a summary of the research design of the study. The table provides a summary of the questions of the study accompanied by the type of data that will be collected and tools that will be utilised to collect data.

A quantitative research strategy can be interpreted as "emphasising quantification in the collection and analysis of data" (Creswell 2007, 6) In contrast, a qualitative research strategy focuses on words in data collection and analysis. The process of induction derives conclusions from collected data to establish a theory. "Qualitative research begins with assumptions, a worldview and the study of research problems inquiring into the meaning individuals or groups ascribe to a social or human problem" (Creswell 2007, 37). This study uses mixed methods, which combine both qualitative and quantitative research strategies. Table 5.1 is a summary of

the research design of the study. It provides a list of the basic questions of the study accompanied by the type of data that is collected and the tools utilised to collect data.

Table 5. 1: Summary of research design

Research question	Data required	Research Method
To what extent do various factors influence user acceptance of information security systems methods in securing and archiving information at UKZN?	Quantitative data	Surveys
To what extent do employee perceptions regarding the information systems security measures at UKZN affect their intention to use information systems security measures?	Quantitative data	Surveys
To what extent do others' beliefs about the use of information systems security measures affect UKZN employee perceptions of and their intentions to use information systems security measures?	Quantitative data	Surveys
To what extent does the current system for archiving academic certificates at UKZN have problems related to employee perceptions of information systems security measures at UKZN?	Qualitative data	Interviews

Questionnaires were administered to UKZN employees in order to test UTAUT factors, and interviews were conducted to check the how the academic certificates are secured and archived at UKZN.

5.6.2 Site of Study

Marshall and Rossman (1999) describe a successful selection of site as one where entry is possible, where the researcher is likely to build trusting relations with the participants in the study, and which allows for good data quality and credibility. UKZN has been chosen because it met the criteria of possible entry, build trusting relations with the participants in the study which will allow for good data quality and credibility. The university consists of five campuses and four colleges, and has an annual intake ranging from 35 000 to 44 000 students. It caters for a high number of students who are from previously disadvantaged communities. UKZN was formed on "1 January 2004 as a result of the merger between the University of Durban-Westville and the University of Natal. The two KwaZulu-Natal universities were among the first batch of South African institutions to merge in 2004 in accordance with the government's Higher Educational restructuring plans that reduced the number of higher educational institutions in South Africa from 36 to 21" (Makgoba and Mubangizi 2010, 3). The university enrols, on average, about 43 000 students every year. It offers both post-graduates and undergraduate studies. The university is situated in the province of KwaZulu-Natal that has a population of about 10 million people. It is the only research-intensive university found in the province. The university graduates on average about 2500 students every year (University of KwaZulu-Natal, Corporate Relations 2016, 1).

5.6.3 Target Population and Sample Frame

The study setting was thus UKZN. The registrar's office, university archives, information communications services department, examination and records department, UKZN auditing firm, qualification verification department and UKZN forensics unit, were participants in the qualitative study. These participants were selected based on their involvement with the degree certificates issued by the university. The participants were interviewed, and the examination and records department received training and a demonstration of how the new system functions. The quantitative sample was drawn from the support services division of UKZN. This division was chosen because it is where most of the archiving, preservation, documentation and securing of critical data takes place within the university.

The support services of the UKZN comprise the following departments: the "UKZN Foundation, forensic services, internal auditing services, corporate relations, legal services, finance, human resources, information communication services, institutional intelligence, IP and technology transfer, quality promotion and assurance, research office, risk management services, student academic administration, student funding centre, and the university teaching and learning office" (University of KwaZulu-Natal, Corporate Relations 2016, 1).

5.6.4 Sampling strategies

The study used the purposive sampling method. Patton (2002) defines purposeful sampling as a method whereby the researcher may select the most informative sample. Merriam (1998) describes purposeful sampling as an information-rich case study. It is for these reasons that the researcher chose to use a purposeful sampling method. The researcher's sample frame consisted only of those employees who were involved or should have been involved in archiving, documentation and preservation of the university's data on the system. Employees who worked within the author's own division were excluded to avoid biasing the survey results.

5.6.5 Sample Size

The following participants formed the qualitative sample: fourteen executive directors, four college managers and other participants who were at the time directly involved with degree certificates from the student academic administration, student records and management, legal services, risk management services, information communication services, forensic unit, internal audit, human resources qualification verification, UKZN Archives, corporate relations and the UKZN Foundation. The quantitative sample was drawn from the support services division of UKZN and limited to those employees who were assumed to be directly involved in archiving, securing, preserving and documenting the university's critical data. This group of employees who have been chosen are not directly involved with the degree certificates, but with the more general aspect of archiving. The qualitative sample is more geared towards the degree certificates. While the support sector employs about 300 employees, about 131 of those employees deal with the general aspect of archiving and securing university data. Therefore, the sample consisted of 131 employees.

5.7 Research Methods and Data Collection Process

5.7.1 Case Study

A case study offers the capacity to the researcher to conduct a comprehensive study of an occurrence "in a real life setting, to inspect issues such as the how and why of the occurrence" (Morgan 1997, 7), (Leo, 1988), (Robson, 2002) and (Yin, 2008). The researcher is unable to influence the outcome. Different data collection methods can be used to gather data within a certain period (Yin, 1994) and (Stake, 1995), and both qualitative and quantitative data can be used to analyse the occurrence under study.

This research investigates UKZN's archival system for academic certificates. There are various divisions within this research and affiliates who will participate. As such, the case study method will be utilised for this research because it is suited to the study.

Three types of case study for research have been identified: "intrinsic, instrumental and collective case studies" (Stake 1995, 4). For this research, an intrinsic case study will be used because it affords the researcher an opportunity to focus on one particular case of the securing and archiving of academic transcripts at UKZN.

5.7.2 Survey

This approach provides the researcher with quantitative data for scrutiny. The data comprises the collective opinions of individuals. Surveys are used in both "cross-sectional and longitudinal studies using questionnaires or a structured interview format. The data is studied and used to generalize findings to a wider context" (Babbie 1990, 8). A survey will be used in the quantitative part of this research. The design of the survey for the study was done on the university system.

Once the design of the survey was complete, a sample survey was sent to ten respondents, and feedback was received. A total of 300 employees work in the division which is responsible for archiving and securing data. An initial email was sent to 130 targeted respondents who are directly involved in the process of archiving and securing information using Innerweb, accompanied by ethical clearance letter, and letter of introduction. A link was distributed the following day to targeted respondents, with the survey questionnaires. After two weeks, a reminder was sent to all the targeted respondents to respond to the survey.

5.7.3 Interviews

Interviews are a means of collecting data using structured and semi-structured questions. Shneiderman and Plaisant (2005) state that interviews are a tool that can benefit research by providing the interviewer an opportunity to pursue and probe a specific question. Genise (2002) highlights the following advantages of the interview method:

- "Few participants are needed to gather rich and detailed data" (Genise 2002, 12);
- The interview is good at obtaining detailed information, and
- The interview allows one-on-one with participants, which normally opens up constructive debates and suggestions sometimes.

Semi-structured interviews allow a researcher to use open-ended questions where deemed necessary and the participant to offer his or her opinion. While questionnaires are good at reaching a wider audience, their weakness is that they cannot be customised to certain individuals. The process of interviews for this study is described next.

The University of KwaZulu-Natal employees who agreed to participate in the study were sent an individual initial request-to-interview invite by email and received a confirming phone call. A date was confirmed with each employee and an appointment was set for the interviews to be conducted face to face. The targeted times were during the lunch breaks of the employees so as not to take them away from their workstations for long periods of time. Most sessions with participants were flexible with time depending on how the participant chose to engage during the process. The proper recording and taking of notes was done after the consent has been obtained from the participant. In an instance where a follow-up interview was needed it was requested at the end of the session.

It was imperative for the researcher to alert the participant that during the interview the entire process will be kept confidential. This process was meant to develop a good relationship with the participant and to assure the participants that they are safe and they must feel secure and engage freely about their social space. “This relationship helps build trust and confidence and gives voice to the participant” (Mishler 1986, 23). A good relationship is not easily achievable in an environment which is not familiar to the researcher. In addition, “it is essential that the researcher understands the context in which the participants express their views, as well as observes any differences during the interviews” (Briggs 1986, 5), (Mishler, 1986). The UKZN participants were given an opportunity to be flexible during the interview process therefore a semi-structured approach was used in the interview process to allow the researcher some level of control over the process.

5.7.4 Grounded Theory

In grounded theory, “a researcher uses the views of the participants to create an abstract theory of a process and action” (Charmaz 2008, 3). “The data collection is divided into multiple stages that assist in the refinement and categorisation to enhance the formulation of a research theory” (Strauss and Corbin 1990, 3), (Charmaz, 2008). This method of research has not been used in the present circumstance because it is not relevant to the study.

5.7.5 Ethnography

"Ethnography is the study of a group of people in a particular environment over a long period" (Wolcott1990, 2). This type of theory involves collecting primary data using interviews and observations. "The research process is flexible and typically evolves in context or response to the realities faced" (Le Compte and Schensul, 1999, 5). This research method is not going to be utilised in this study as it is not fit to the type of the study being done.

5.7.6 Instruments and Data Collection

In this study questionnaires were used for the survey and an interview guide was used for the interview questions. For the survey questions, participants were required to respond to items specifically to do with performance expectancy, effort expectancy, social influence and facilitating conditions, with gender, age, experience and voluntariness of use as moderators. Respondents were asked to rate items on a four-point Likert scale according to their level of agreement with the statements: strongly disagree (1), slightly disagree (2), slightly agree (3) or strongly agree (4). The study formulated Likert scale questions on a 4-point basis so as to prevent users from choosing the neutral option. The survey and interview questions were piloted first to ensure validity. These items were adapted from various published sources. The semi-structured questions, intended to investigate existing processes for the securing and archiving academic transcripts at UKZN, were in the form of an interview guide.

5.8 Data Quality Control

5.8.1 Measurements

A quantitative study is relatively easy to evaluate for credibility by using measures of reliability and validity. However, for a qualitative study, a trustworthiness strategy can be used. Creswell (2007) claims that trustworthiness in qualitative research can be verified by using credibility, transferability, conformability and dependability as indicators. The researcher will be using this strategy for qualitative data, and reliability and validity for the quantitative data.

5.8.2 Data Analysis

"Qualitative data analysis involves dividing data into manageable units, coding, synthesizing and searching for patterns" (Bogdan and Biklen 2003, 8). Yin (2003) also emphasises that data analysis is a search for patterns. It deals with large amounts of data that must be sorted, indexed

and interpreted so as get a meaningful conclusion. The selected approach to data analysis should help facilitate an understanding of the issues of handling academic certificates and challenges related to the processes. Therefore, the analysis here will include four phases: quasi-statistical analysis, editing, immersion and thematic analysis (Crabtree and Miller, 1992).

The final phase, thematic analysis, itself includes several steps: “coding the material; identifying themes; constructing thematic networks; describing and exploring thematic networks; summarising thematic networks and interpreting patterns” (Attride-Stirling 2001, 391). The data analysis process will assign thematic codes to the responses.

The quantitative data will be analysed using the statistical software package SPSS, to describe statistics, including frequencies, means and standard deviations.

5.9 Case Study Description

The university’s management is aware of the current challenges and potential issues surrounding certificates and fraud, particularly as some of the reported cases took place at the university. The goal of the university is to increase the level of efficiency and develop quality systems to archive and handle academic certificates. In 2016, a British company, Advanced Secure Technologies, approached the university. They provide a secure document system that enables universities to issue and verify both laser-printed and electronic documents in a one-click process. Their system includes an online application to allow graduates to view their degree documents and to grant permission to third parties, such as employers, to verify their degree documents in a self-service online process, www.advancedsecure.co.uk. However, the university opted to engage a thorough study of the security and implementation processes. Hence, this research will address the following research questions:

- To what extent do various factors influence user acceptance of information security systems methods in securing and archiving information at UKZN? To what extent do employee perceptions regarding the information systems security measures at UKZN affect their intention to use these measures?
- To what extent do others’ beliefs about the use of information systems security measures affect UKZN employee perceptions of and intentions to use information systems security measures?

- To what extent does the current system for archiving academic certificates at UKZN have problems related to employee perceptions regarding the information systems security measures at UKZN?

The questions were asked during the interviews. Each group of participants received different set of questions. The qualitative questionnaires are attached in appendix G.

5.9.1 Interviewee Group 1: The Registrar

"The Registrar's Office is a nerve centre upon which the support to the governance and academic administration of the University revolves carrying out its work under the guidance of the strategy of the University and its Council" (University of KwaZulu-Natal, Corporate Relations 2016, 3). "The Portfolio has four directorates, namely, Student Academic Administration; Governance and Administration; Legal Services; and Risk Management Services. The functions of the Registrar's Portfolio include, but are not limited to, providing administrative, legal and secretarial services to the University Senate, Council, Convocation and the Executive Management of the University. The Portfolio is also responsible for the dissemination, implementation and maintenance of
University-wide policies, procedures and systems" (University of KwaZulu-Natal Corporate Relations 2016, 3). "The registrar's operational duties are as follows:

- Provision of administrative and secretarial service to Senate, Council, Convocation and the Executive Management. This is achieved through the work of Committee Services, i.e. taking, recording, disseminating and retaining minutes of meetings, ensuring managed and effective access to information and records.
- Protection of University against legal risks by ensuring the development and implementation of procedures, rules and guidelines for drawing up of legal agreements and ensuring that all legal agreements and contractual relationships (other than those related to human resource and research issues) are screened and vetted by the legal adviser.
- Administering centralised policies, procedures, systems and information data-banks (other than those pertaining to financial or human resource matters) by disseminating and maintaining rules of procedures, and ensuring that the University complies with all copyright requirements" (University of KwaZulu-Natal Corporate Relations 2016, 3).

5.9.2 Interviewee Group 2: Student Records

"The Department of Student Academic Administration (SAA) supports the vision, mission and values of the university by providing effective and efficient service to staff, current and prospective students". (University of KwaZulu-Natal website 2016, 51).

"It strives to uphold high levels of accountability, professionalism and innovation. SAA provides the following academic support functions across the five campuses of the university:

- Processing student enquiries and applications.
- Coordinating the interface between the university and Central Applications Office.
- Preparing undergraduate and postgraduate prospectus and college handbooks.
- Administering examinations.
- Maintaining student records.
- Preparing lecture and exam timetables and handling venue bookings" (University of KwaZulu-Natal website 2016, 51).

5.9.3 Interviewee Group 3: Forensic Unit

"In an effort to prevent fraud at UKZN, a forensic services division was formed. The primary role of the division is to prevent, detect and respond to fraud risk within the university. This is done by implementing a 24-hour toll-free, tip-off anonymous whistle-blowing facility, which is managed by an outside company and may be used to anonymously report fraudulent activities within the university" (University of KwaZulu-Natal website 2016, 5). The division has a fraud policy and response plan which defines fraud risk and the university's response thereto. There is also a whistle-blowing policy that sets out the manner in which allegations of suspicious activities may be reported (University of KwaZulu- Natal, Corporate Relations 2016, 3).

5.9.4 Interviewee Group 4: Internal Audit

The internal auditors support and enable the university in realising its vision and mission, in line with global best practices and sound governance, without fear or Favour. The internal audit's values are to engender, through interactions with all stakeholders, the values of sound governance based on ethical principles of fairness, accountability, responsibility, transparency, respect, professionalism, integrity and confidentiality (University of Kwazulu-Natal, Corporate Relations, 2016).

5.9.5 Interviewee Group 5: Risk Management Services

The purpose of Risk Management Services is to create an attractive and competitive environment for UKZN by ensuring an experience for students, staff and visitors, that is professional, safe and secure. Risk Management Services provides a 24-hours-a-day, 365-days-a-year service with the objective of creating an environment that is conducive to working and living, teaching and learning and conducting research on the premises of the university (University of KwaZulu-Natal, Corporate Relations, 2016).

5.9.6 Interviewee Group 6: Archives

The University Archives collects, appraises, organises and preserves unique and historical records, reflecting the history of the University from the time that it was established. It serves as the official memory of the University and consists of a wide variety of materials. The Archives preserves and ensures the accessibility of records of permanent value. It aims to provide an effective and efficient information service to patrons. The material at the University Archives reveals "the origin and development of the University from 1910 when the Natal University College (NUC) was established, through the years of the former University of Natal (1949-2003), to the present-day University of KwaZulu-Natal. In 2004, the University of Natal merged with the University of Durban-Westville to form the University of KwaZulu-Natal. The collection covers both the Pietermaritzburg (PMB) and Durban campuses (Howard College and Medical School) and more recently, publications from the Edgewood and Westville campuses" (Makgoba and Mubangizi 2007, 6).

5.9.7 Interviewee Group 7: Information and Communication Services (ICS)

"The information and communication services division (ICS) is the amalgamation of ICT, DMI and AV Departments. ICS strives to become more efficient by assuming the prime responsibility for the planning, development, and maintenance of the University of KwaZulu-Natal. The division works closely with the user community in providing an array of services to support and leverage to the academic, student and administrative endeavors of the institution" (University of KwaZulu-Natal, Corporate Relations 2012, 3).

5.10 Summary

This chapter discussed the research methodology in general, the chosen methods as well as the reasons for why they were appropriate choices for the study. The chapter also discussed the

benefits of the chosen research strategy and how it fits within the study context. Criteria for the UKZN case study selection were discussed and supported. The chapter also outlined the data collection process which was utilised in the study. The next chapter provides an analysis of the quantitative survey data collected at UKZN.

CHAPTER 6

DATA ANALYSIS

6.1 Introduction

This chapter presents the results of a quantitative survey. The quantitative surveys were conducted as a measure of how employees in the field of securing and archiving information feel about the information security systems. The survey was to assist in providing perspective on the following questions of the study:

- To what extent do various factors influence user acceptance of information security systems methods in securing and archiving information at UKZN?
- To what extent do employee perceptions regarding the information systems security measures at UKZN affect the intention to use information systems security measures?
- To what extent do the beliefs of others about the use of information systems security measures affect UKZN employee perceptions and the intention to use information systems security measures?

6.2 Survey Results

A total of 300 employees work within the divisions under the study; however, 131 employees were selected for the study as they are directly involved in securing and archiving information at the University of KwaZulu-Natal. The survey was emailed to them. There were 131 responses, of which 35 were partially complete and 96 were complete. In order to ensure that all the employees who were sent a link did open it, a number of physical visits were conducted every week to those participants who were not responding. This was followed by daily phone calls.

“Statistics is a set of procedures and techniques used to collect, organize and analyse data, which are the basis for making decisions in situations of uncertainty” (Mann 2005, 2). The field of statistics is divided into descriptive and inferential. The statistical data of this study were subjected to the following tests in performing the analysis:

- “Descriptive statistics, which consists of methods for organizing, displaying, and describing data by using tables, graphs and summary measures” (Mann 2005, 3).

- Chi-square goodness-of-fit-test: “In a goodness-of-fit-test, it tests the null hypothesis that the observed frequencies for an experiment follow a certain pattern. The test is called a goodness-of-fit test because the hypothesis tested is how good the observed frequencies fit a given pattern” (Mann 2005, 526). Thus, out of 131 responses 96 were complete, this means the results were a good representation to use in observing frequencies and pattern in order to arrive at a conclusion.
- Wilcoxon Signed Ranks test: A non-parametric test used to test, in this study, whether the average value is significantly different from a value of 2.5 (the central score). This is applied to Likert scale questions. It is also used in the comparison of the distributions of two variables.
- Spearman’s correlation: Correlations measure how variables or rank orders are related. The 96 completed responses represent a sufficient response which will allow the correlations measure to perform the rank orders of the variables. The presentation is divided into six broad sections. Section One will focus on demographic data; Section Two will look at performance expectancy; Section Three will analyse effort expectancy; Section Four will focus on social influence; Section Five will be on facilitating conditions and Section Six will be on the behavioural intention to use.
  Later, the analysis will explore the inter-relationships between some of these sections.

6.3 Quantitative Analysis for Different Data Types

The following tests were applied when reporting results: a Wilcoxon signed rank test which tests for significant agreement or disagreement, the mean agreement score (M), the test statistics (Z) and the p-value. P-value output given as .000 is unique to SPSS. It means that the p value is very small. Therefore, the results do not give the exact p value if it is <.0005. It is customary to report p values that show as .000 in SPSS as p <.0005. By definition, a category with a percentage occurrence >50% is termed a majority. Output from SPSS gives test statistics to 3 decimal places and that is the reporting format adopted in this study.

6.3.1 Demographic Data

In Table 6.1, the responses reflect that the majority of the respondents think that archiving and securing information is part of their job. This is statistically supported by a reflection of a significant number of the sample (80-84.21%), who indicated that they think archiving and securing information is part of their job, $\chi^2(1) = 42.667$, $p < 0.0005$.

Table 6. 1: Archiving and securing

Answer	Count	Percentage
Yes (Y)	80	84 21%
No (N)	20	15. 79%

In Table 6.2, the responses reflect that the majority of the respondents have good computer knowledge. It is statistically significantly that more than expected (65-68.42%) rated their computer knowledge as 'good', $\chi^2(2) = 51.063$, $p < 0.0005$.

Table 6. 2: Computer knowledge

Answer	Count	Percentage
Very little	0	0. 00%
Fair	14	14. 74%
Good	65	68. 42%
Expert	16	16. 84%

As shown in Table 6.3, the responses reflect that the majority of the respondents are familiar with the Innerweb system 77 - 81.05, $\chi^2(2) = 94.938$, $p < 0.0005$.

In Table 6.4, it is seen that the majority of respondents are end users of the system. This means they access the system to action certain tasks in their daily operational activities, unlike those who are the administrators of the system.

Table 6. 3: Familiarity with Innerweb

Answer	Count	Percentage
Uploader of information	5	5, 26%
End user of the system	65	68, 42%
Both of the above	25	26, 32%

Table 6. 4: Task performed on Innerweb

Answer	Count	Percentage
Uploader of information	5	5, 26%
End user of the system	65	68, 42%
Both of the above	25	26, 32%

As summarised in Table 6.5, the responses suggest that the majority of respondentsaccess Innerweb once in a while. A significant number of the sample (41, 43.16%) indicated that they do so, $\chi^2(3) = 22.250$, $p < 0.0005$.

Table 6. 5: Frequency access of Innerweb

Answer	Count	Percentage
Every day	20	21,05%
Once in a while	41	43,16%
Seldom	26	27,37%
Not sure	8	8,42%

Table 6.6 shows that the majority of respondents, over the previous 6 months, spent less than an hour on the system when logged on. The sample has 51, 53.68% who indicated that when they are logged into Innerweb, it is mostly for less than an hour, $\chi^2(2) = 18.813$, $p < 0.0005$.

Table 6. 6: Average time logged onto Innerweb

Answer	Count	Percentage
Less than an hour	51	53, 68%
More than an hour	28	29, 47%
None	16	16, 84%

As shown in Table 6.7, the majority of respondents logged on to the Innerweb for less than an hour. The sample. significantly reflects that 67, 70.53% indicated that they spend less than an hour logged onto the Innerweb, $\chi^2(2) = 60.063$, $p < .0005$.

Table 6. 7: Average time spent on Innerweb

Answer	Count	Percentage
Less than an hour	67	70,53%
More than an hour	8	8,42%
Not sure	20	21,05%

In Table 6.8, it can be seen that the majority of respondents have been working for the University of KwaZulu-Natal for more than five years. The statistics reflect that a significant number of the sample (22, 23.16%) indicated that they have worked at the University, $\chi^2(2) = 94.938$, $p < 0.0005$.

Table 6. 8: Years of employment at the university

Answer	Count	Percentage
Less than a year	8	8,42%
Between one and five Years	22	23,16%

Table 6.9 shows that the majority of respondents were female.

Table 6. 9: Gender of respondents

Answer	Count	Percentage
Female	51	53, 68%
Male	44	46, 32%

As shown in Table 6.10, the majority of respondents were 41 years and older. Table 6. 10: Your Age

Answer	Count	Percentage
21 years and below	0	0,00%
Between 22 and 40 years	37	38,95%
41 years and above	58	61,05%

In this section, demographic data was presented. The age, gender and knowledge about the the Innerweb were shown by various tables. The next section presents the

6.3.2 Performance expectancy of the respondents.

6.3.2.1 Performance Expectancy

The overall summary of performance expectancy is reflected in Figure 6.1. It reflects an overall positive agreement on how using the Innerweb will facilitate positive outcome in the tasks.

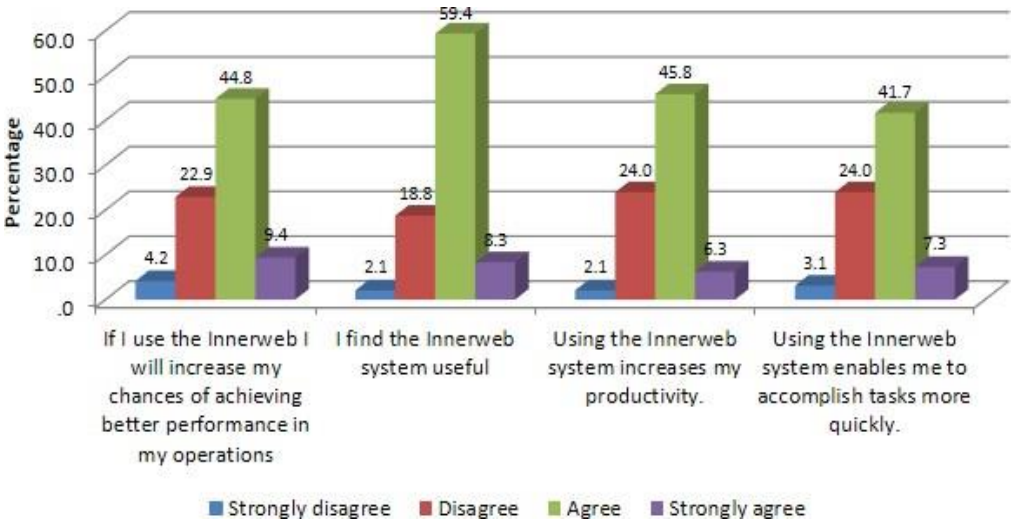


Figure 6. 1: Performance Expectancy.

Table 6.11 shows that the majority either agree or strongly agree that the Innerweb system increases their chance of achieving better performance in their operations. There is significant agreement that using the Innerweb will do so, $M = 2.73$, $Z = -2.833$, $p = 0.005$.

Table 6. 11: Correlation between Innerweb and performance

Answer	Count	Percentage
Strongly disagree	4	4, 21%
Disagree	22	23, 16%
Agree	43	45, 26%
Strongly agree	9	9, 47%
N/A	17	17, 89%

The responses in Table 6.12 reflect that the majority of respondents find the system useful. The statistics support that statement, $M = 2.84$, $Z = -4.723$, $p < 0.0005$. Table 6. 12: Innerweb usage

Answer	Count	Percentage
Strongly disagree	2	2, 11%
Disagree	18	18, 95%
Agree	57	60, 00%
Strongly agree	8	8, 42%
N/A	10	10, 53%

The responses, summarised in Table 6.13, show the majority believe that using the system increases their productivity. There is significant agreement that using the Innerweb will do so, $M = 2.72$, $Z = -2.907$, $p = 0.005$.

Table 6. 13: Correlation between Innerweb and productivity

Answer	Count	Percentage
Strongly disagree	2	2,11%
Disagree	23	24,21%
Agree	44	46,32%
Strongly agree	6	6,32%
N/A	20	21,05%

Table 6.14 shows that the majority of respondents believe that using the system enables them to accomplish tasks more quickly, $M = 2.70$, $Z = -2.450$, $p = 0.005$.

Using the Innerweb system enables me to accomplish tasks.

Table 6. 14: Correlation of Innerweb and accomplishment of task

Answer	Count	Percentage
Strongly disagree	3	3,16%
Disagree	23	24,21%
Agree	40	42,11%
Strongly agree	7	7,37%
N/A	22	23,16%

This section presented the data analysis of performance expectancy for the respondents on using the Innerweb at UKZN. The majority of responses were in the strongly agree to agree categories on the chances of improving performance in operations, being useful, increasing productivity, as well as helping with quicker accomplishment of tasks.

6.3.2.2 Effort Expectancy

The summary of the overall effort expectancy is reflected in Figure 6.2. The effort expectancy reflects that there is a majority agreement that learning to operate the system is easy and clear.

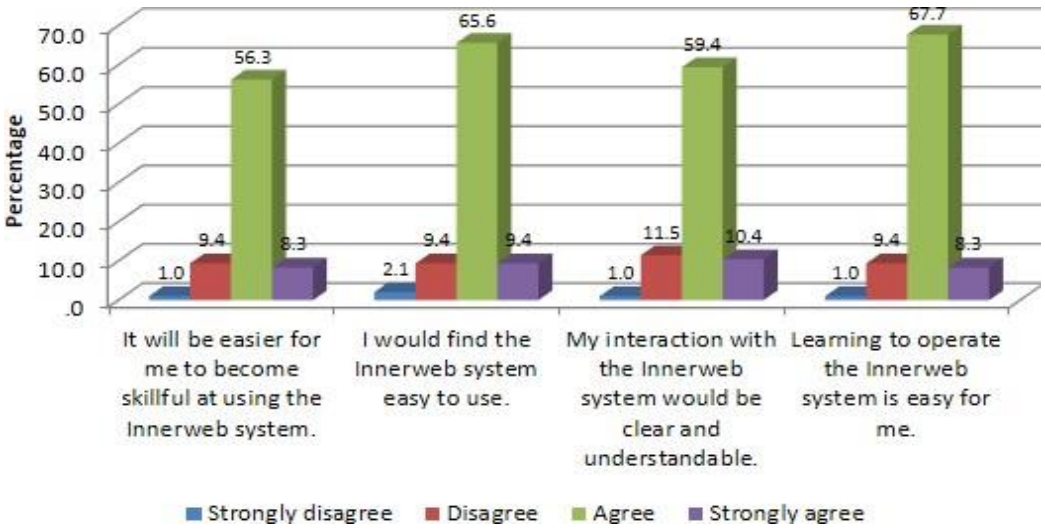


Figure 6. 2: Effort Expectancy.

In Table 6.15, it can be seen that the majority of respondents feel it will be easy for them to become skilled at using the system. The statistics support that becoming skilled at using the Innerweb will be easier, M = 2.96, Z = −5.881, p = .005.

Table 6. 15: Correlation between Innerweb and skills

Answer	Count	Percentage
Strongly disagree	1	1,05%
Disagree	9	9,47%
Agree	54	56,84%
Strongly agree	8	8,42%
N/A	23	24,21%

Table 6.16 shows that the majority of respondents felt they would find it easy to use the Innerweb system. There is significant agreement that they would find it to be so, M = 2.95, Z = −6.237, p = 0.005. In Table 6.17, the summarised responses show that the majority would find interaction with the system to be clear and understandable There is significant agreement that they would find it to be so, $M = 2.96$, $Z = -5.996$, $p = 0.005$.

My interaction with the Innerweb system would be clear and understandable.

Table 6. 16: Correlation between Innerweb and usability

Answer	Count	Percentage
Strongly disagree	2	2,11%
Disagree	9	9,47%
Agree	63	66,32%
Strongly agree	9	9,47%
N/A	12	12,63%

Table 6. 17: Correlation between Innerweb and interaction

Answer	Count	Percentage
Strongly disagree	1	1,05%
Disagree	11	11,58%
Agree	57	60,00%
Strongly agree	10	10,53%
N/A	16	16,84%

In Table 6.18 it can be seen that the majority of responses reflect that learning to operate the system is easy. There is significant agreement that it is indeed easy, $M = 2.96$, $Z = -6.628$, $p = 0.005$.

Table 6. 18: Innerweb operation

Answer	Count	Percentage
Strongly disagree	1	1, 05%
Disagree	9	9, 47%
Agree	65	68, 42%
Strongly agree	8	8, 42%
N/A	12	12, 63%

This section presented the data analysis of effort expectancy for the respondents on using the Innerweb at UKZN. The majority of responses agree that it will be easy to be skilled, understand and learn to operate the Innerweb.

6.3.2.3 Social Influence

The overall summary of the social influence is reflected on the Figure 6.3. The social influence reflects that in general, there is a good organizational support on the use of the Innerweb system.

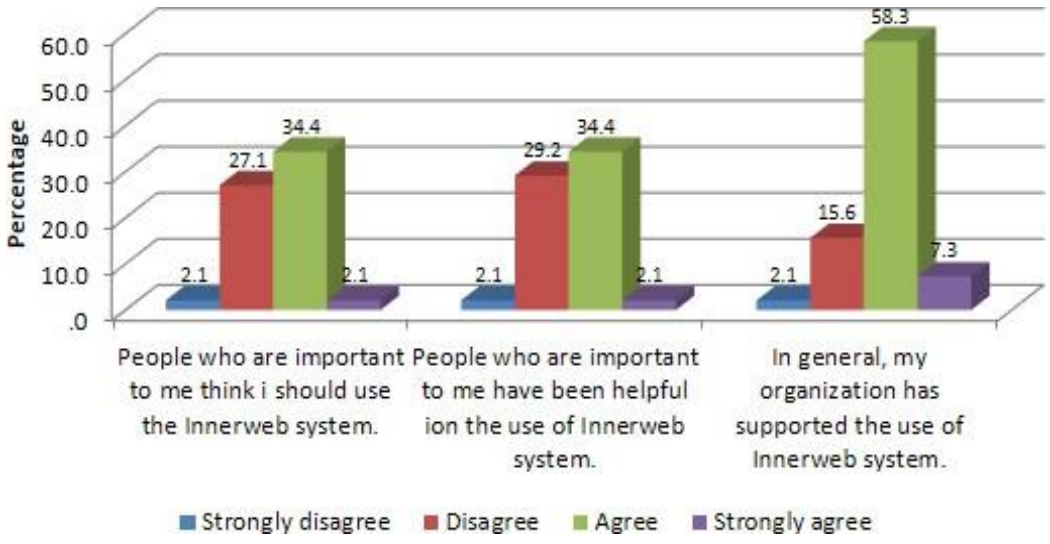


Figure 6. 3: Social Influence

In Table 6.19, the responses reflect other people's influence on respondents use of the system. There is agreement that people who are important to the respondents think that the Innerweb system should be used, $M = 2.56$, $Z = -.804$, $p = .005$. However, it should be noted that a sizable number of respondentsanswered 'not applicable'. This could be attributed to respondents whose jobs do not require an influence from other people to perform their task.

Table 6. 19: Correlation between Innerweb and people influence

Answer	Count	Percentage
Strongly disagree	2	2, 11%
Disagree	26	27, 37%
Agree	33	34, 74%
Strongly agree	2	2, 11%
N/A	32	33, 68%

In Table 6.20, the summarised responses reflect an equal perception of how people who are important to respondents have been helpful with respect to use of the Innerweb system. There is significant agreement that they have been helpful with regard to using the system, $M = 2.54$, $Z = -.567$, $p = 0.005$. However, it should be noted that a sizable number of respondents answered'not applicable'. This could be attributed to respondents whose jobs do not require an influence from other people to perform their task.

Table 6. 20: Correlation between Innerweb and helpful people

Answer	Count	Percentage
Strongly disagree	2	2,11%
Disagree	28	29,47%
Agree	33	34,74%
Strongly agree	2	2,11%
N/A	30	31,58%

Table 6.21 shows that the majority of respondents believe the organisation has supported use of the system, with statistically significant agreement, M =2.85, Z = −4.891, p = .005. In general, the organisation has supported the use of the Innerweb system

Table 6. 21: Correlation between Innerweb and organization support

Answer	Count	Percentage
Strongly disagree	2	2,11%
Disagree	15	15,79%
Agree	56	58,95%
Strongly agree	7	7,37%
N/A	20	20,00%

This section presented the data analysis of social influence for the respondents on using the Innerweb at UKZN. The majority of responses agree that the organization has supported the use of the Innerweb.

6.3.2.4 Facilitating Conditions

The overall summary of the facilitating conditions is summarized in Figure 6.4. The facilitating conditions reflect an overall agreement in the availability of the needed tools in facilitating the use of the Innerweb.

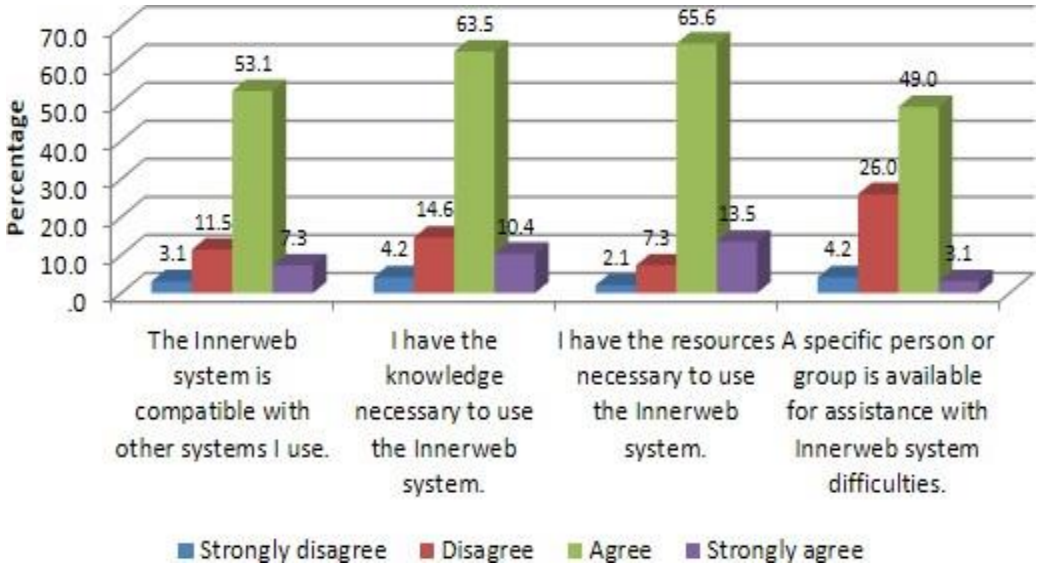


Figure 6.4: Facilitating conditions

The responses summarised in Table 6.22 reflect that the majority of respondents agree that the Innerweb system is compatible with other systems they use. It is confirmed statistically that there is significant agreement that the previous statement is true., M = 2.86, Z = −4.676, p = 0.005. As shown in Table 6.23, the majority of respondents have the knowledge necessary to use the system, which statistically shows significant agreement that they do, M =2.87, Z = −5.055, p = 0.005.

Table 6. 22: Compatibility between Innerweb and other systems

Answer	Count	Percentage
Strongly disagree	3	3,16%
Disagree	11	11,58%
Agree	51	53,68%
Strongly agree	7	7,37%
N/A	23	24,21%

Table 6. 23: Correlation between Innerweb and knowledge necessary to use it

Answer	Count	Percentage
Strongly disagree	4	4,21%
Disagree	14	14,74%
Agree	61	64,21%
Strongly agree	10	10,53%
N/A	6	6,32%

Table 6.24 shows that the majority of respondents feel they have the resources necessary to use the Innerweb system, with. statistical confirmation, M = 3.02, Z = −6.718, p = 0.005.

Table 6.25 shows that the majority of respondents feel there is a specific person or group available for assistance with any system-related difficulties. This is confirmed by statistics which reflects the significant agreement that there is a person or a group of people available to assist with the systems problems, $M = 2.62$, $Z = -1.969$, $p = 0.005$.

Table 6. 24: Resources for use of Innerweb

Answer	Count	Percentage
Strongly disagree	2	2,11%
Disagree	7	7,37%
Agree	63	66,32%
Strongly agree	13	13,68%
N/A	10	10,53%

Table 6. 25: Innerweb service assistance

Answer	Count	Percentage
Strongly disagree	4	4,21%
Disagree	25	26,32%
Agree	47	49,47%
Strongly agree	3	3,16%
N/A	16	16,84%

This section presented the data analysis of facilitating conditions for the respondents on using the Innerweb at UKZN. The majority of responses agreed that they have resources and knowledge necessary to use the Innerweb. They have found the Innerweb to be compatible with other systems, and at times when there were difficulties, assistance was available.

6.3.2.5 Behavioural Intention to Use

The overall summary of the behavioural intention to use the Innerweb is summarized in Figure 6.5. The behavioural intention reflects the overall agreement in predicting, intending and planning to use Innerweb system in the future.

In Table 6.26, it can be seen that the majority of respondents expect to use the system in the future. This is reflected in the statistical analysis that there is significant agreement that the majority of the respondents predicted that they will use the system in the future, $M = 2.91$, $Z = -5.473$, $p = 0.005$.

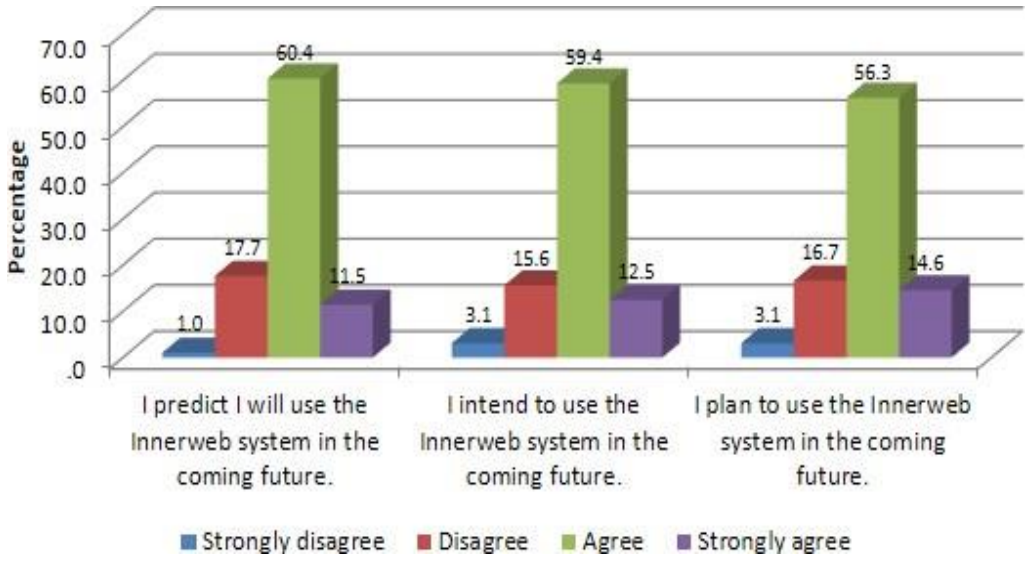


Figure 6. 5 Behavioural intention to use

Table 6. 26: Prediction of future Innerweb use

Answer	Count	Percentage
Strongly disagree	1	1,05%
Disagree	17	17,89%
Agree	58	61,05%
Strongly agree	11	11,58%
N/A	8	8,42%

Table 6.27 shows that the majority respondents intend to use the system in the future, which is statistically confirmed by the significant agreement that most respondents intend to use the system in the future, $M = 2.90$, $Z = -5.143$, $p = .005$ Finally, Table 6.28 reports that the majority of respondents plan to use the system in the near future. Statistically, there is an agreement that the majority of the respondents are planning to use the Innerweb in the future, $M = 2.91$, $Z = -5.032$, $p = .005$.

Table 6. 27: Intention to use Innerweb in the future

Answer	Count	Percentage
Strongly disagree	3	3,16%
Disagree	15	15,79%
Agree	57	60,00%
Strongly agree	12	12,63%
N/A	8	8,42%

Table 6. 28: Planning to use Innerweb in the future

Answer	Count	Percentage
Strongly disagree	3	3,16%
Disagree	16	16,84%
Agree	54	56,84%
Strongly agree	14	14,74%
N/A	8	8,42%

This section presented the data analysis of behavioural intention to use the Innerweb at UKZN. The majority of respondents agree that they are planning, intending and predicting on using the Innerweb in the future.

6.4 Inter-relationship

The correlation, coefficient following analysis with spearman's correlation to test for linear relationships between two ordered variables. There is a strong positive correlation between performance expectancy and Behavioural Intention to use the system, $\rho = .553$, $p < .0005$.

In other words, the agreement that the system will assist performance is correlated with agreement that they intend to use the system. Analysis reveals that there is a positive correlation between effort expectancy and behavioural intention to use the system, $\rho = 0.413$, $p < .0005$. This therefore confirms that there is an agreement that effort expectancy will assist the behaviour agreement to use the system. In a relationship between social influence and behavioural intention to use the system, there is a positive strong correlation, $\rho = 0.543$, $p < .0005$. It is concluded that social influence plays a positive role in the behavioural intention to use the system. There is a strong positive correlation between facilitating conditions and behavioural intention to use the system, $\rho = 0.361$, $p < .0005$. Therefore, the facilitating conditions will contribute positively to a behavioural intention to use the system. The illustration in Figure 4.1 of the UTAUT model depicts the links from performance expectancy, effort expectancy, social influence and facilitating conditions to behavioural intention and user behaviour, with experience, voluntariness, age and gender as moderating factors.

6.5 Summary

The survey set up to answer the following questions:-

1). To what extent do various factors influence user acceptance of information security systems measures for securing and archiving information at UKZN?

2). To what extent do University of KwaZulu-Natal employee perceptions regarding the information systems security measures at UKZN, affect their intention to use these measures?

3). To what extent do others' beliefs about the use of information systems security measures affect UKZN employee perceptions of and intentions to use these measures?

The analysis of the survey examined various factors that influence users to accept information security systems to answer the first research question: to what extent do various factors influence user acceptance of information security systems measures for securing and archiving information at UKZN? The facilitating conditions reflect an overall agreement in the availability of the needed tools in facilitating the use of the innerweb system. Furthermore, social influence reflects that there is good organizational support on the use of innerweb system. The survey also reviewed employee perceptions of systems security measures and how it affects

their intentions to use information systems security measures in order to answer the second research question: to what extent do University of KwaZulu-Natal employee perceptions regarding the information systems security measures at UKZN, affect their intention to use these measures?. The effort expectancy reflects that there is a majority agreement that learning to operate the system is easy and clear, and performance expectancy reflects that there is a positive agreement on how the innerweb will facilitate positive outcome in the tasks.

Others' beliefs influence the use of information systems security measures by UKZN employees and were surveyed in order to answer the third research question: To what extent do others' beliefs about the use of information systems security measures affect UKZN employee perceptions of and intentions to use these measures? The behavioural intention reflects overall agreement in predicting, intending and planning to use the innerweb system in the future.

CHAPTER 7

QUALITATIVE ANALYSIS OF THE INTERVIEWS

7.1 Introduction

The qualitative analysis will be done using Nvivo word cloud and word tree. According to Feng and Behar-Horenstein (2019), "Nvivo allows researchers to analyse open-ended responses to survey and interview questions as well as other text data like reflective writing, image and videos" (Feng and Behar-Horenstein 2019, 563). Nvivo is a data management system that allows a researcher to make sense of textual data under scrutiny.

This section is going to start by reporting on the open-ended questions which were part of the quantitative survey. The survey ended with an open-ended question. The question asked the respondents to say anything they feel will be relevant to the survey. The analysis of the open-ended questions was done using thematic codes.

Qualitative interviews were conducted in order to answer the 4th research question of the study: To what extent does the current system used to archive academic certificates at UKZN have problems related to employee perceptions of the information systems security measures at UKZN?

Interviews were conducted with 14 respondents, addressing the 4th research question and their responses are presented below.

7.2 Open-ended Questions

The open-ended questions theme codes are presented and discussed using the Nvivo software. In order to establish the key terms mentioned by the respondents in the survey, a Word Cloud was generated using Nvivo Pro version 12. The prominence of the word 'Innerweb' is clear, given that it is the main key word around which the survey was organised. Some words which were mentioned include 'users', 'simple', 'information', 'system', 'policies', and 'software'. These elements characterise an information platform. In the context of this survey, these could be what the respondents expected the system to deliver or what they knew the system is meant to deliver.

Figure 7.1 shows this intuitive characterisation by the respondents of the innerweb. In this figure, the depiction confirms that the questions that were answered were all related to the innerweb. The tree further reveals what was expressed in the open-ended questions about the innerweb. The bigger words are a reflection of what was the main focus of respondents and the smaller words are what might have been mentioned during the survey but not carrying as much weight.

Figure 7.1: Intuitive characterization of Innerweb

Respondents were asked to add any comments concerning the Innerweb. Only 15 of the 131 respondents commented. Traditionally, respondents do not respond to these open-ended questions. The responses can be characterised as mixed. Some respondents were positive and others negative, while yet others were ambivalent. It is not clear whether to attribute the non-responses either as negative or ambivalent. The responses confirm what falls between the continuum from positive to negative and encompass responses in between the two extremes. For example, a respondent might say: 'The innerweb is not user friendly and to me, there is no support or FAQs or help button to assist the user. It is often not clear how to search the innerweb to find information' (Respondent 5, End-user).

The utility of the Innerweb was questioned by some. The following excerpts encapsulate these sentiments:

'Does not serve an important function - could be utilised more effectively' (Respondent 13).

‘Not very user friendly. It could be made simpler (Respondent 13).

There are items that need to be updated on a regular basis. When a system is perceived as not being user-friendly, its usefulness, efficiency and effectiveness are questioned. Consequently, propositions that indicate its redundancy are also made as the quotes suggest.

On a positive note, a respondent said: ‘Automated systems are better than manual systems provided there is flexibility in the systems’ (Respondent 15).

The value of a system can be found in its flexibility, as the comment suggests. This in some way implies the rigidity inherent in manual systems which are susceptible to, for example, human error and human subjectivity. Others find its user-value, as shown in the following excerpt:

‘It is useful and its hands-on program. But I recommend we have people ready to assist when having difficulties in the pool that we have available to us’ (Respondent 59).

In the same vein, a respondent said: ‘I use the Innerweb for academic software’s and putting university notices where necessary’ (Respondent 135, End-User).

Those who know how the system works reflect satisfaction in its purpose and functionality. Other respondents offered advice on how the system can be improved, such as by providing a ‘How to use the Innerweb’, which must be made available at all times and embedded in the system. One respondent (15) was blunt and suggested that the ‘System needs replacement’.

Some level of frustration was expressed by a respondent (number 5) who observed that ‘The innerweb is too secretive. Nobody knows what it contains. Finding information is difficult and the search function is really poor. Keep the options simple and limit the navigation to six tabs (Information, Applications, Software, Policies, and so on). Make the user interface straightforward and simple to use.’

Simplicity is a virtue that makes systems user-friendly. As a result of the ‘unfriendliness’ of the Innerweb, it has become somewhat obscured and regarded as ‘secretive’.

Some of the respondents expressed ignorance regarding its functionality and purpose. The following excerpt is illustrative:

‘I am not familiar with the system and not sure what purpose it serves since ITS is available as an application used University wide’ (Respondent 6).

The respondent, like others, insinuated duplication and redundancy given the existence of the ITS system.

Another respondent said: ‘First time I am hearing about innerweb. More training or workshop on the subject would be recommended’ (Respondent 7).

This also emphasises the level of ignorance prevalent among people who are sup- posed to use the system for their benefit. A system is as good as its contents.

A respondent observed: ‘The innerweb is not user friendly and yet we are supposed to use is as a source of policies. The policies are outdated, which make this system useless’ (Respondent 46).

A respondent was resigned to not using it: ‘I no longer use this site. Instead it points to other websites which I normally type in manually which is why I no longer use it’ (Respondent 8).

Figure 7.2 shows a word tree, also generated using Nvivo Pro version 12. The sentiments from respondents are clear: it is not clear how to use it, and there is a need to train users undergirded by user guidelines in order to debunk and demystify its secretiveness and user-unfriendliness.

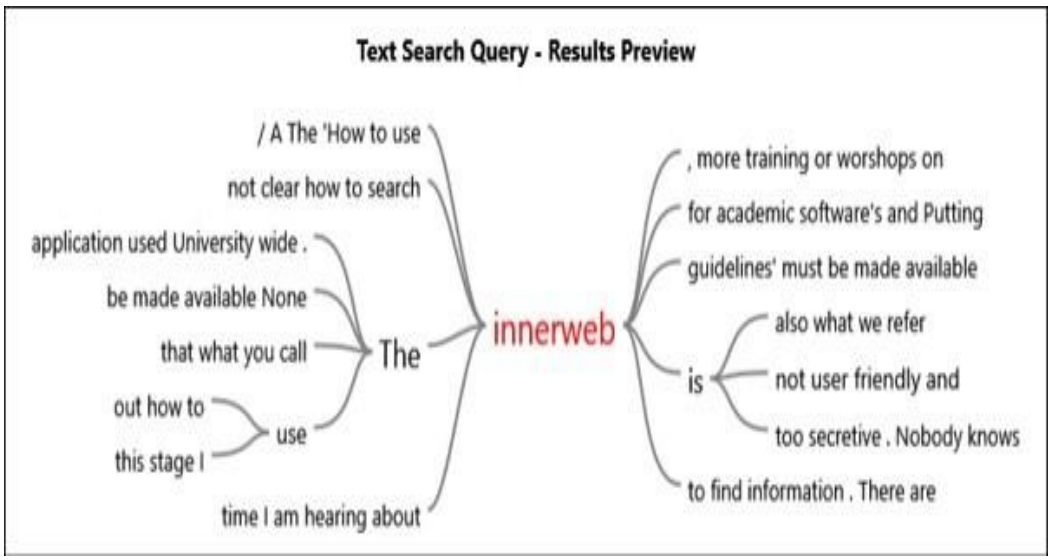


Figure 7.2: Wordtree

7.3 General Observations

The purpose of the survey was to provide a perspective on various factors that influence user acceptance of information security systems methods in securing and archiving information at UKZN. The survey was to also look at employee perception and other’s beliefs on information security measures, as well as how they affect their intention to use information systems security measures. The word tree figure 7.2 below is a reflection of open-ended question which reflects that the innerweb system is not user friendly, and that training on how to operate is needed.

This word tree could be linked to the behavioural intention to use the system, which could be summarised to reflect an intention and planning to use innerweb system in the future once training and workshop has been received.

7.4 Archiving and Securing Academic Certificates

Participants: the UKZN Registrar's Office, Examination and Records Department.

7.4.1 Job Content: Description by Participants

One of the participants worked in the Registrar's Office, Student Records and Examination Department of the university, while the rest worked in student records in the Colleges of Humanities; Law and Management; Health Sciences and Agriculture, Engineering and Sciences.

7.4.2 Processes of Archiving Academic Certificates

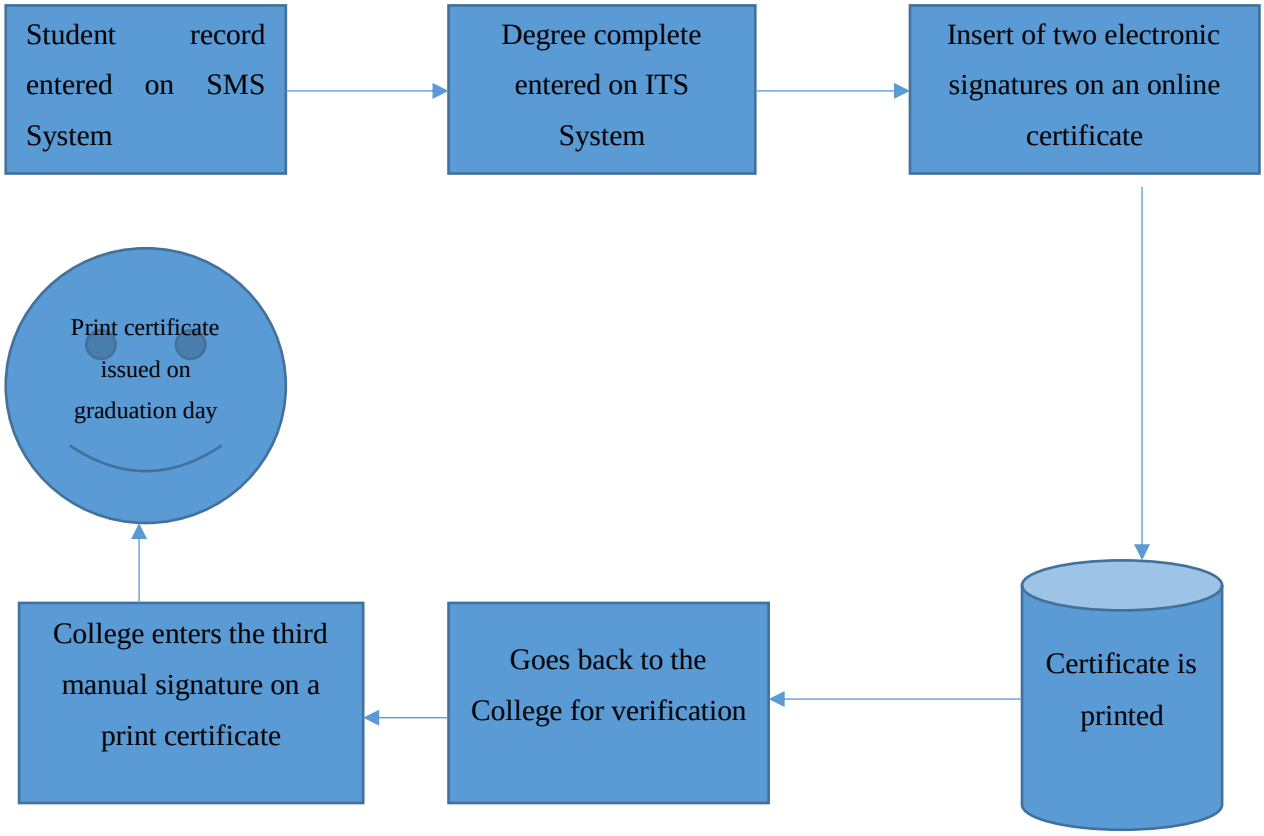
Participants were asked whether their section archives academic certificates. Most of the participants were of the view that there is no practice of archiving of academic certificates. Only one of the participants narrated some process although they acknowledged the absence of a permanent archival procedure being in place, as shown in the following excerpt: "From my knowledge of archiving there is no permanent archiving in place but there is a process in place but which does not store data permanently".

The process which is currently in place is as follows:

- Administrators first enter the data of a student on the Student Management Services (SMS)
- Administrators enter degree completed on the Integrated Technology Services system (ITS)
- Student Records and Examination Department harvest completed degrees on ITS
- Student Records insert two electronic signatures, those of the Vice-Chancellor and Registrar
- Student Records print certificates

- Student Records and Examination Department send the printed certificates to the Colleges for the third signature of the Dean and Head of School (which is a safety feature)
- Colleges return the certificates to Student Records and Examination Department
- Student Records and Examination Department issues print certificates to a graduand during a ceremony (during the graduation, Student Records scan the student number of those present who are able to collect the certificates).

Process chart flow 7.1



Another participant was blunt and said, in response to the question 'To what extent does the current system used to archive academic certificates at UKZN have problems related to employee perceptions of the information systems security measures at UKZN?': "Not that I know of". The respondent's answer reflected that she could not relate to the expectation of what the university expects from her. This goes against the UTAUT model with respect to attributes such as performance expectancy and behavioural intention. This, however, could be explained by the absence of the facilitating conditions at UKZN as provided in the UTAUT model. The

answer reflects that though these questions were meant to address the qualitative question, they addressed the quantitative survey questions.

7.4.3 Archiving Records of Graduates

Participants were asked whether their section/institution archives records of the graduates. One of the respondents was forthright: What is in place is the ITS system which keeps data of all students who graduated from this university. The data contains who the student is, when did they graduate, what degree they graduated with and the courses they did and when they were completed and their personal details". This suggests the existence and use of an Information Technology (IT) system at UKZN, with capacity to store and retrieve data, that is fit for purpose. This was affirmed by the other participants who acknowledged the adoption, acceptance and use of such a system. One of the participants emphatically said: "Yes, the ITS system of the university does!", which resonated with other responses.

7.4.4 Software used to Archive Academic Certificates and Records of Graduates

Participants were also asked about the software that was used to archive certificates and records of the graduates. This question was important to verify the level of awareness regarding the available software systems. Knowledge of the systems is important for facilitating adoption and use. All the participants responded that the available software packages specific to academic certificates were ITS and SMS, which are, interestingly, different from Innerweb.

There was a small percentage of participants in the Innerweb survey who indicated that they had no knowledge of the Innerweb. This however could be attributed to the absence of facilitating conditions.

7.4.5 Duration of Use of Software

Experience with the software is important for efficiency. Participants were asked the length of time they had been using the software. For many, it was familiarity from inception, as the following excerpts confirm: "Since I started working for the university, but the second software is new"; "Since employment"; "From the time I started my portfolio", and "Since I started working here". Access to the software was granted from inception.

7.4.6 Previous Software Used

Knowledge of the previous software is critical for the adoption of new software. Participants were asked if there was any software they used before using the software currently in place. All participants revealed no knowledge of the old software.

7.4.7 Person Responsible for the Existing Software

Participants were asked about their knowledge of the person or department responsible for the technical problems of the software. This question was critical to understand how the facilitating conditions enable the participants. Many participants (%) responded that it was ICS responsibility to attend to technical problems of the system. ICS has a 4000 call which is responsible for resolving all the technical problems.

7.4.8 Person Responsible for Archiving Data on the Current Software

The knowledge within an organization about systems flow is very important. Participants were asked about who carries the responsibility of capturing data on the software. Participants from the different colleges explained that they were responsible for the data capturing of their own colleges, which flows to the Registrar's Office, Student Records and Examination Department for a signature; the data then flows back to the colleges for the final signature and to be ready for final printing.

7.4.9 Software Technical Problems

Participants were asked about the challenges encountered with the current software. Though most participants had not encountered any problems with the software, one participant did indicate that she had encountered problems with the software.

7.4.10 Software problem solutions

The participant who voiced encountering a problem with the software were asked to detail the problem encountered and the solutions implemented. The participant stated that the problems encountered were to do with the systems being down, as well as information not being captured correctly. The ICS then provided solutions.

7.4.11 The strength and weaknesses of the Software

Participants were asked to elaborate on the functionality of the software, both good and bad. Most participants (80%) expressed the view that the system has been working well; however, a few (10%) participants raised their concerned about the incapability of a system to permanently store data. This was to do with the possibility of a graduand losing the original certificate with three signatures, as the re-print does not have three signatures but two.

7.4.12 Additional Points on Archiving of Academic Certificates on the Software

The participants were asked to make additional points about what they thought was relevant to the system. One participant highlighted the fact that recent changes at the university is proof that it takes the safety of the degree certificates seriously, as staff are currently working on adding more security features on the certificates. He further mentioned that he thought it was going to be wise to keep a photocopy of every original certificate issued, since it contains all features.

7.5 The Process Flow

Participants: ICS, Examination and Records Department

7.5.1 Flowchart for Archiving Academic Certificates

There was one respondent here. The participant was asked to detail the process flow of archiving academic certificates. The participant responded that there was no archival system in place for academic certificates. He mentioned that the process which was in place did not store the academic certificates. Instead, the system keeps the basic records of a student who graduated from the university.

7.5.2 Authorized Access

The participant was asked to outline the authorized access to the basic records of the student. He stated that the Student Records and Examination Department is authorized to have access to the records.

7.5.3 Alternative Authorized Access

A question was asked about the alternative authorized individual who has access. The participant observed that the ICS Department takes the responsibility of granting temporary access to the person next in charge so that he or she has access.

7.5.4 Authorized Generated Notification

The participant was asked to detail the process in place regarding the transparency of the system. The participant mentioned that the ICS system keeps logs of all staff members' access time, place and data, time spent on the system, as well as records retrieved. The ITS system is widely used. It has a number of modules, and one of those modules handles student records. It is a technologically advanced system that records all activities, including who logged in, when and where. It is easy to track all activities which have occurred on the system, as it has a back-up storage facility.

7.6 Replacement of a Lost Student Record

Participants: Student Records and Examination Department

7.6.1 Certificates Requisition

The question asked the participants to detail the process in place for students when requesting a reprint of a certificate.

The participants explained that the student must produce an identity document when requesting a certificate, then Student Records and Examination Department check and verify the details of the student on the ITS system. Student Records then print a certificate with two electronic signatures and finally, the certificate is handed to the student. However, participants from the colleges described their system a little differently: when the students come to them, they get referred to the Student Records and Examination Department as the department is responsible for the reprint.

7.6.2 Information Retrieval

The respondents were asked about the person responsible for retrieving student records on the system. All participants agreed that it was the responsibility of Student Records and Examination Department.

7.6.3 Alternative Information Retrieval

On the question of the alternative person to do information retrieval, many participants explained that there have never been such reported cases. However, they believe that students make prior arrangements and if the right person is not available, there will be an acting staff member in place.

7.6.4 Academic certificates software

Participants: Forensic Unit, UKZN Qualification Verification Department, UKZN auditing firm.

7.6.5 Participants Responsibility

Participants were asked to outline their responsibilities in the process of archiving certificates. The first respondent works in the Forensic Unit of the university, which is responsible for, amongst other things, the fraud and misuse of university information or properties. The second Respondent works in the auditing unit of the university, which is responsible for the audit of all the issued academic certificates and the process flow.

The third respondent works in the Human Resources Department of the university, which is responsible for the verification of the academic certificates of potential employees and employed staff.

7.6.6 Safety features

Respondents were asked if they had knowledge of the safety features of archived records being compromised. All participants agreed that they have had to deal with the safety features of the archived records being compromised.

7.6.7 Safety features compromised

Participants were asked to elaborate on how the safety features of the archived records ever came to be compromised. They all responded with their unique stories. The first participant gave a scenario where there was a case that was discovered through the media, on the university's academic certificates. The types of cases that were investigated in the past primarily revolved around external parties forging degree certificates and submitting these to prospective employers purporting to be issued by the university. According to the participant, the incidents were largely outside university control and investigations were merely requested by complainants to criminally prosecute such offenders. However, the university records did not agree with what was purported to have happened resulting in the forged degree certificates. The university authorities brought this to the attention of the participant for thorough investigation, findings and recommendations.

Another scenario was an internally reported matter from one of the university departments that was to do with what was believed to be a case of tampering with the features of the academic certificate. The second participant emphasized that though there was never a direct reporting of the incident since employment, that through the files of the university there have emerged some cases which suggest that activities of fraud had been reported in the department and were investigated accordingly.

The third participant chose to protect the identities of individuals and opted to generalize in the answers by mentioning that during the interview processes, there have been cases where they were trying to verify the existence of an academic qualification from potential employees, which upon investigation, produced negative results, suggesting that the qualification did not exist.

7.6.8 Solutions to Tampering with Safety Features

The participants were asked to provide comment on how they dealt with those problems they came across. The first participant responded by saying that with both scenarios, what was followed was the proper forensic investigation processes, which was to uncover the truth, conclude the case and make recommendations to senior management of the university. The second participant mentioned that whenever the department received cases like these, the

criminal part is referred to the Forensic Unit and their department is responsible for investigating the system processes which might have led to problems and then to make recommendations for improvement. The third participant noted that the potential employer was notified of the discovery and was allowed to make recommendations which were then relayed to the potential employee.

7.7 Additional Comments

The participants were asked to add information they felt was relevant to the research. The first participant made a recommendation based on the university experience relevant to the division, that a repository of degree certificates at the university will provide great enhancement. With the governance and oversight required, it would place the credibility and integrity of university degrees in high esteem and will provide assurance to any oversight structures at the university, such as the Audit and Risk Committee and Council, that university degree certificates remain authentic and highly respected.

The second and third participants were both tasked by the University to investigate a secured method of securing certificates, recently attended a workshop organised by the UK based company on securing certificates. The workshop was held at the University of Johannesburg.

They provided a detailed step by step recommendation to assist the UKZN in securing their certificates which as follows:-

The security of the print paper for the certificates should consist of the following security features to protect against fraudulent and counterfeit.

The features that protect against fraudulent alteration

- Watermarked security certificate paper
- Microtext (extra fine)
- Validate number
- Heat reactive spot
- Hologram
- Audit number
- Toner secure
- Bespoke hologram overprint
- Corporate numismatic security design

- Micro-numismatic invisible UV (anti-tamper technology)
    - controlled material
    - genuine multi-tone watermark
    - cannot be reproduced in a printing process
    - provide high-level protection against counterfeiting
    - difficult to accurately colour copy or scan
    - random number unique to each certificate
    - website document authentication
    - Invisible UV Ink
    - Cannot be reproduced by colour copying or laser printing
    - instant certificate authentication (on reverse)
    - controlled material
    - design cross matches to watermark design
    - provides high level protection against counterfeiting
    - a unique 8 digit auditrac number is applied to each certificate at point of production
    - this audit number provides ongoing customer control of physical certificate stocks
    - advanced toner paper adhesion
    - provides high-level protection against alteration of the laser print
    - personalised with your logo/brand
    - prevents hologram tampering
    - enhances hologram security
    - personalised to your corporate name/login
    - created with high level banknote graphic software
    - extremely difficult to reinstate/counterfeit
    - provides high level protection against alteration of the laser print
    - unique security graphics technique called micro-numismatics
    - guards against fraudulent alteration and counterfeiting
    - protects every character of personalisation infill
    - Easy to detect fraud
    - Virtually impossible to re-instate
    - guards against fraudulent alteration and counterfeiting

The verification of qualifications should ideally be managed and controlled in-house by institutions

- not shared with 3rd party vendors
- always up to date
- available online
- fast and easy to use
- reliable and trusted by external users
- cost effective

There should be an online web portal for graduates which is:-

- self-service portal for graduates and employers to verify qualifications
- online portal for all graduation records request for re-printing of certificates (including online payments and courier)
- issue electronic academic records or transcripts

It should be noted that in these listed features, only 30% of the features currently exist in the certificates. Further to that, the current ITS system is proof that someone has a particular certificate. This means the records could be changed. However, for the crtificates to be protected there needs to be actual proof. This is because the original certificate is the only one that gets three signatures, where one of the signatures is inserted manually.

The fourth participant highlighted that since UKZN is a leader in research, it is important that the systems are proactive rather than reactive. The reason is that there is always going to be a potential criminal who wants to try to exploit loopholes in the systems. The participant further mentioned that there is a need to be always ready to deal with such criminals, through up-to-date systems which are constantly reviewed.

The fifth participant responded that archiving academic certificates might help with verification purposes, where one simply pulls the archived copy out and does a comparison. It might also help with the processes of auditing. Possible weaknesses of the ITS system that might compromise data were noted as follows: during the replacement process for a lost certificate, only two signatures are needed instead of three. Staff responsible for entering data may alter or falsify information. A student may fake a certificate that is similar to the original. Additionally, the university is in the process of adding more safety features to its hard-copy certificates to make them difficult for intruders to copy.

The recommendations which were repeated by interviewees are highlighted next.

- First recommendation: It would be wise to keep a photocopy of every certificate issued to preserve all original features.
- Second recommendation: A repository of degree certificates at UKZN could enhance governance through robust record keeping; it would maintain the credibility and integrity of UKZN degrees and provide assurance to oversight structures at UKZN, such as the Audit and Risk Committee and Council, that the degree certificates remain authentic and highly respected.
- Third recommendation: Archiving might help for verification purposes, allowing users to pull out the archived copy and compare. Archiving might also help with the processes of auditing.

7.8 Theorising Records

Using Nvivos Word Tree, it is possible to postulate some key elements related to the records. Based on the interview responses, the following elements are important to note: **access, collaboration, authority, safety, notifications and breach.**

To elaborate, **access** is important for users, as without it they are not able to use the records. However, that access should not be unfettered but controlled.

Collaboration is encapsulated in working with others. This is essential for the integrity of the records and the establishment of smooth workflows in an environment that requires confidentiality and the safety of records.

Safety is crucial for the credibility of the records and the institution as a whole and is important for accountability.

Authority and its hierarchies bestow the power to execute the production of records at various levels of the organisation, both in terms of the vertical and horizontal hierarchies.

Notifications are enablers for prompting actions in an IT-based record- keeping environment and should be embedded in the system.

Breach is invoked when offences are committed through the hacking or faking of documents, which implies that systems must be infallible and failsafe, as steganographic embedding capacity would allow. This is illustrated in Figure 5.8.

The Word Cloud in Nvivo shows the relative importance of words expressed during the interviews by the relevant respondents in the study, the participants. Words such as ‘Records’, ‘Responsible people’, ‘Structures’, ‘Certificates’, ‘Students’ and ‘Information’ were important. Regarding the size of words in the Word Tree, the larger the word, the more frequently it was mentioned. The more frequently the word was mentioned, the more their relative importance.
This is illustrated in Figure 7.2.

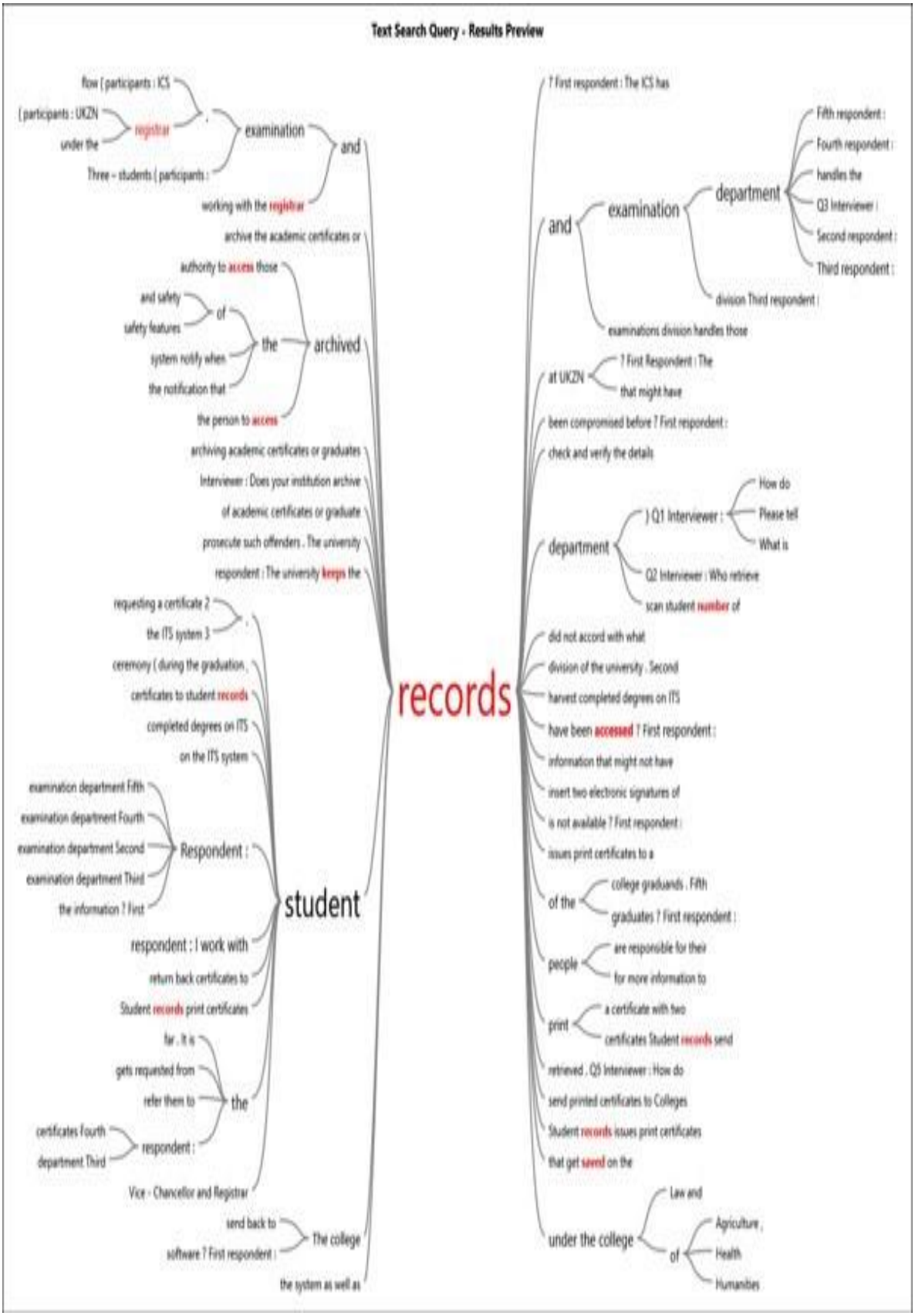


Figure 7. 1: Nvivo Hierachy chart

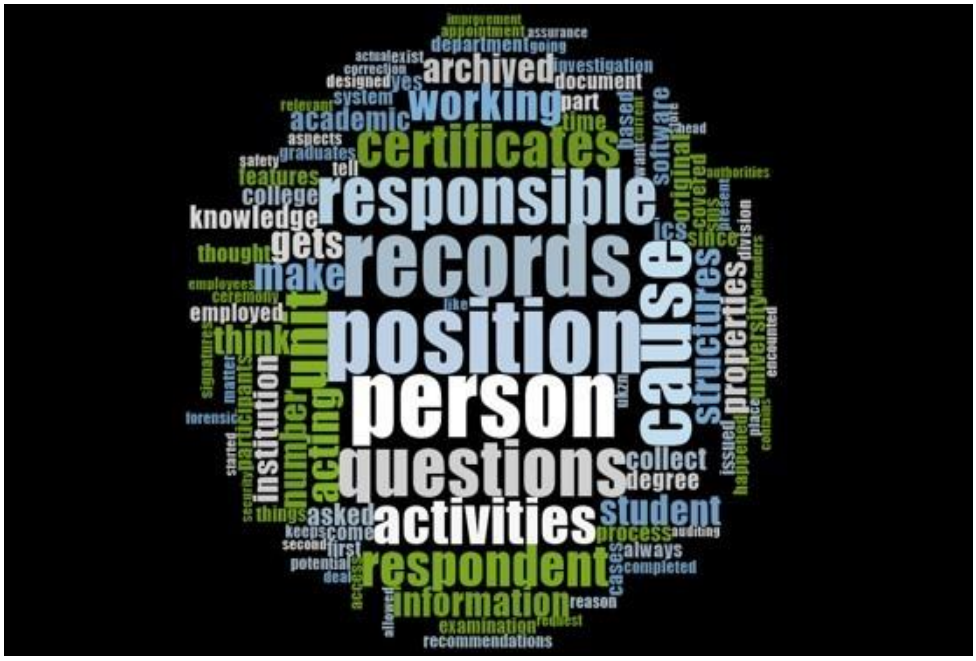


Figure 7. 2: Nvivo Word Cloud

7.9 Summary

The qualitative interview results have been presented in this chapter. The qualitative results revealed that while there are software systems in place to secure academic certificates, at this stage, the software is not used to permanently archive documents in the university. The results further outline the process in place currently and offered recommendations for the development of a system that will protect and archive academic certificates. Against this backdrop of the results obtained, the following chapter discusses in detailed the software system developed to actually undertake the protection of the archived content.

CHAPTER 8

DISCUSSION OF THE FINDINGS OF QUANTITATIVE AND QUALITATIVE ANALYSIS

8.1 Introduction

Mixed methods research is defined as a method that "draws upon the strengths and perspectives of each method, recognising the existence and importance of the physical, natural world as well as the importance of reality and influence of human experience" (Johnson and Onquegbuzie, 2004 in Ostlund et al., 2011, 370). It is thus a method that draws on the strengths from both the quantitative and qualitative perspectives.

(Tashakkori and Creswell 2007, 3) "define mixed methods research as research in which the investigator collects and analyses data, integrates the findings and draw inferences using both qualitative and quantitative approaches". However, it should be noted that the combination of both qualitative and quantitative data may not only bring advantages as there may also be disadvantages.

In a "mixed methods study, the idea of mixing qualitative and quantitative methods should be made known in order to establish how the analytic techniques relate to one another and how if at all, the findings should be integrated" (O'Cathain et al., 2008, 5 in Ostlund et al., 2011, 370). It helps the study if the purpose of using both qualitative and quantitative methods is outlined from the beginning and the possible advantages are given.

8.2 Triangulating complementary results

In this study, the qualitative data complemented quantitative data on the level of awareness on the software systems to be used to archiving and securing information at UKZN.

The qualitative data revealed that there was an awareness regarding the available software system to archiving and securing data. Participants mentioned ITS and SMS as the specific software systems used for archiving and securing academic certificates. The majority of the respondents on the quantitative data revealed that they were familiar with the Innerweb system which is for archiving and securing information.

In this qualitative study, participants mentioned that the department called ICS was responsible for technical problems of the system for archiving and securing academic certificates. These results were supported by the quantitative survey results, where the majority of the respondents believe the organisation has supported the use of the system.

The results of the qualitative and quantitative empirical data confirms that there is a complementary triangulation between qualitative and quantitative results on the user acceptance of the system at UKZN. Figure 8.2 below illustrates the use of triangulation on complementary results of the UKZN respondents.

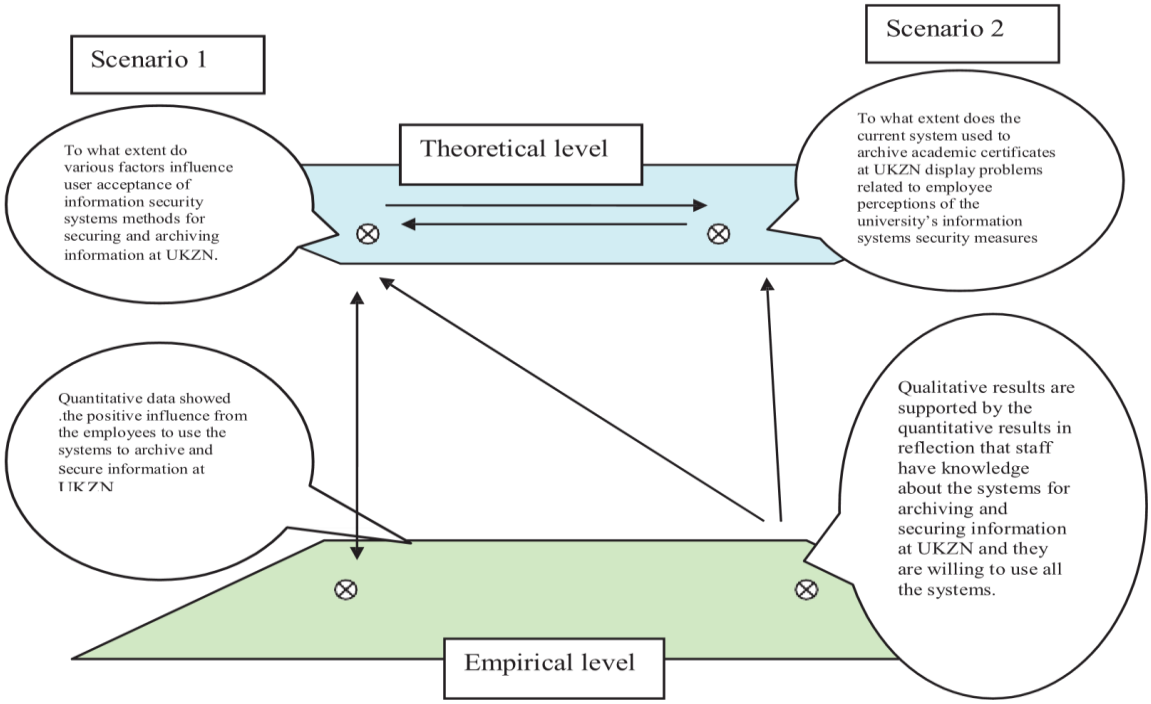


Figure 8.2 "Illustrating the use of triangulation" (Erzberger and Kelle, 2003) on complementary results of the UKZN respondents on the user acceptance of the systems.

The complementary results build on the original triangulation diagram which depicts how theoretical data could be supported by the empirical data. In this triangulation, the theoretical data of qualitative and quantitative complemented the empirical qualitative and quantitative data. This validates that what has been claimed in the theory can be confirmed by the empirical findings; furthermore, the qualitative data support the quantitative data.

8.3 Triangulating convergent results

The qualitative results which were derived from Nvivo's Word Tree, reflect how the respondents ranked what they perceived to be important about the archiving and securing the academic certificates. The respondents raised the inter-relationship between what they identified as enablers in their positive use of the system. The access, collaboration, safety, authority, notification and breach must all work in synchrony with the positive intention of using the system.

Access is ranked as important: without access, the users will not be able to see the records. Collaboration is cultivating the culture of working with others. Safety is critical when accessing records. The qualitative findings supplement the UTAUT constructs by showing strong positive correlation between performance expectancy and Behavioural Intention to Use the system.

The quantitative survey inter-relationship results reflect positive correlation on all levels between behavioural intention to use the system with other constructs. It is the strongest on performance expectancy, followed by effort expectancy, then social influence and facilitating conditions. All of these constructs agree positively with the behavioural intention to use the system. The ranking of correlations are as follows:-

- Strong positive correlation between performance expectancy and Behavioural Intention to Use the system,
- Positive correlation between effort expectancy and behavioural intention to use the system,
- Positive correlation between social influence and behavioural intention to use the system,
- Strong positive correlation between facilitating conditions and behavioural intention to use the system.

Figure 8.3 below illustrates the use of triangulation on convergent results.

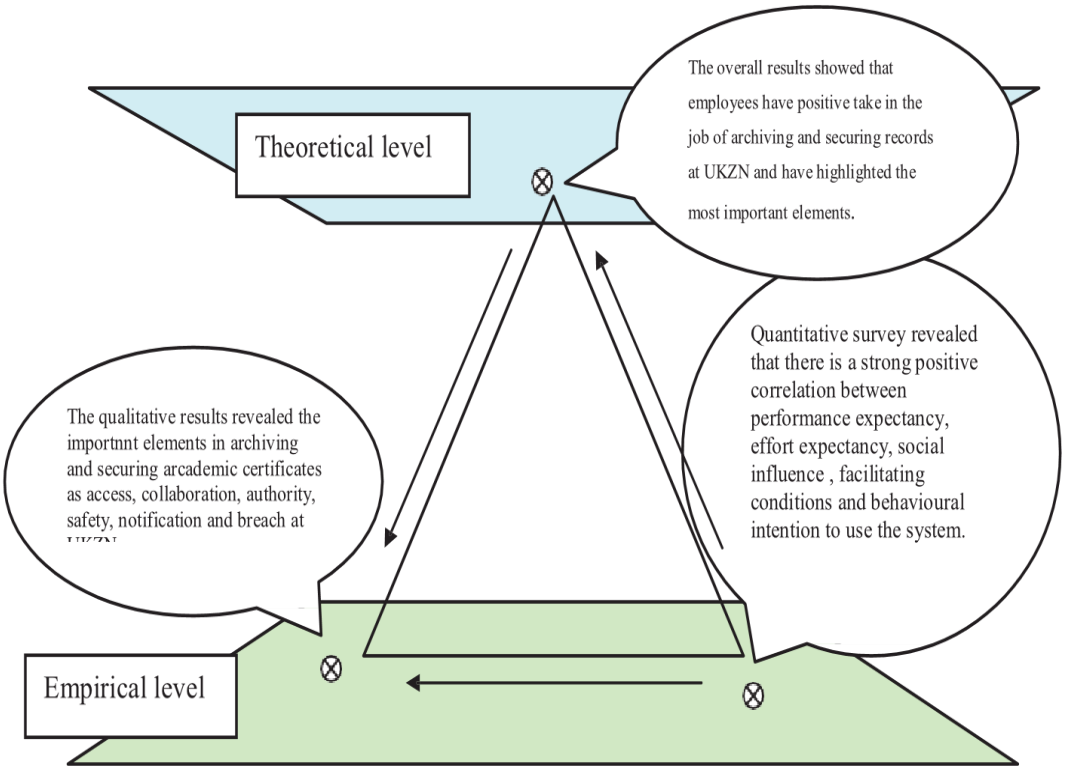


Figure 8.3 Illustrating the use of triangulation (Erzberger and Kelle, 2003) on convergent results of the UKZN respondents on the user acceptance of the systems.

8.4 Triangulating divergent results

The results of an open-ended question in the quantitative survey revealed that the majority of the participants did not have positive comments about the system Innerweb, when compared to the questions about the knowledge of the system for qualitative results. Respondents were asked to add any comments concerning the Innerweb. Only 15 of the 131 respondents commented. Most participants who responded expressed frustrations with the system. Examples of the responses of the respondents are as follows:

The innerweb is not user friendly to me, there is no support or FAQs or help button to assist the user. It is often not clear how to search the innerweb to find information' (Respondent 5, Enduser).

A contrast was found for the qualitative interviews in Questions 7.7.1 and 7.7.2, where participants expressed having knowledge of the system in archiving records of graduates and in terms of the software used to archive academic certificates and records of graduates.

8.4.1 Archiving Records of Graduates

Participants were asked whether their section/institution archives the records of the graduates. One of the respondents was forthright:

What is in place is the ITS system which keeps data of all students who graduated from this university. The data contains who the student is, when did they graduate, what degree they graduated with and the courses they did and when they were completed and their personal details.

This establishes the existence and use of an Information Technology (IT) system at UKZN, with capacity to store and retrieve data, that is fit for purpose. Such a view was affirmed by the other participants who acknowledged the adoption, acceptance and use of the system.

8.4.2 Software used to Archive Academic Certificates and Records of Graduates

Participants were also asked about the software that was used to archive the certificates and records of the graduates. This question was important to verify the level of awareness regarding the available software systems. Knowledge of the systems is important for facilitating adoption and use. All the participants responded that the available software packages specific to academic certificates were ITS and SMS, which are, interestingly, different from the Innerweb.

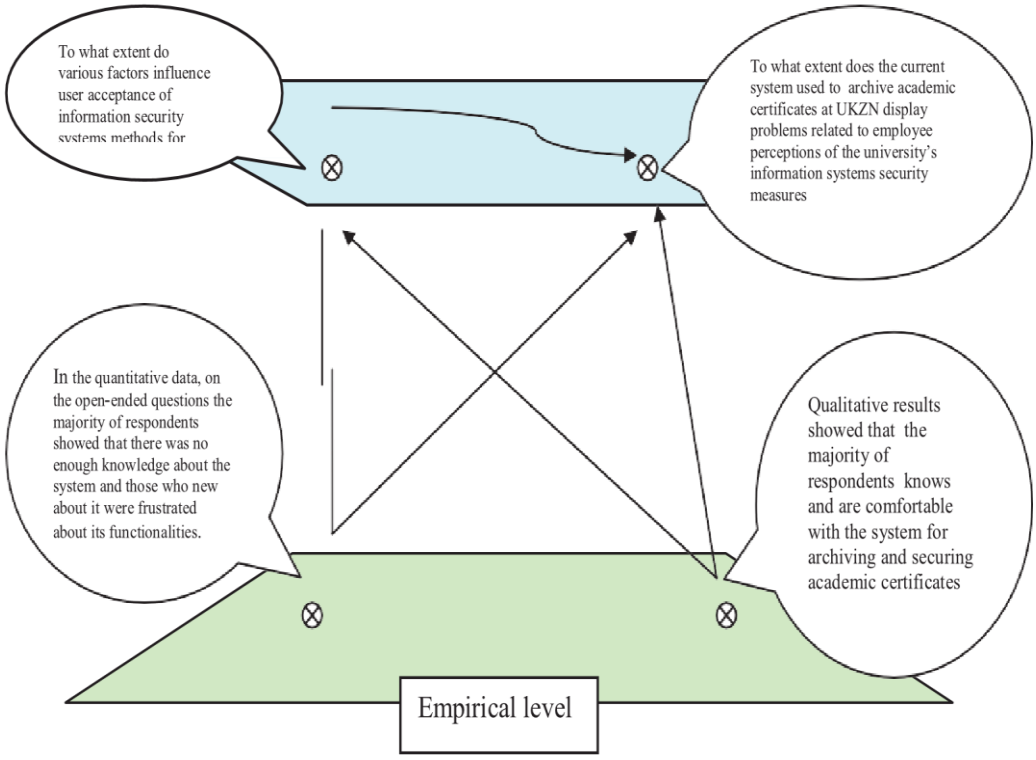


Figure 8.4 Illustrating the use of triangulation (Erzberger and Kelle, 2003) on divergent results of the UKZN respondents on the user acceptance of the systems.

8.5 Triangulating to develop theory

The results to the question to what extent the current system used to archive academic certificates at UKZN displays problems, related to employee perceptions of the university's information systems security measures, showed that the employees perceived the system as one that they needed and they used it willingly, despite all the challenges which were revealed by the participants. Figure 8.5 below illustrates the use of triangulation to develop a theory.

In Chapter 4, theories were discussed. In Gregor (2006) the two definitions which are significant on exploring and expressing what theories are firstly, theory as statement of relationships among constructs that can be tested, and secondly, theory as a statement which indicates how something should be done in practice. The first statement was supported by Davis (1986 in Gregor 2006, 613), when he introduced the technology acceptance model which is based on two particular beliefs: that the user perceived usefulness and ease-of-use, which are of relevance for computer acceptance behaviour. This is a theory which leads to testable propositions. Therefore, the quantitative survey results did support the Davis theory of the technology acceptance model, which was later upgraded to UTAUT, confirming that there is a link between performance expectancy, effort expectancy, social influence and facilitating conditions, and behavioural intention to use the system, with experience, voluntariness, age and gender as moderating factors with UKZN respondents.

The theory as a statement which indicates how something should be done in practice, was supported by Davis and Olson (1985 in Gregor 2006, 613). They stated that this means that a theory in information systems communicates the way in which management information systems should be designed, implemented and managed.

Meanwhile, Siponen and Baskerville (2018) pointed out that information system security management is one area which shows a substantial gap between theories used and practical intervention, which is witnessed by daily reports of information systems security and privacy breaches.

In the qualitative interviews, the employees revealed that there was a need for an automated system to deal with the permanent archiving and securing of the academic certificates. The

respondents further provided detailed features of how a perceived new system should be. This new knowledge which came from the qualitative interviews helps to build a theory.

Therefore, the qualitative interviews enhanced the quantitative results by highlighting and further addressing the gap of the lack of sufficient practical interventions which then forms the starting point for building a theory on how constructs are related, as the results of UTAUT model on quantitative data are enhanced by the qualitative data results.

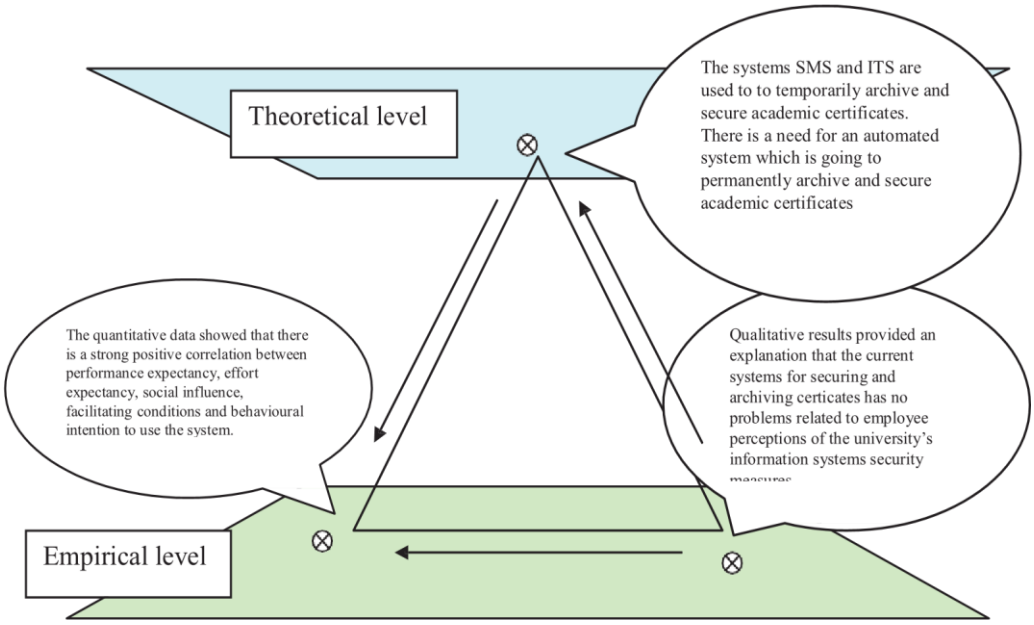


Figure 8.5 Illustrating the use of triangulation (Erzberger and Kelle, 2003) to develop theory of the UKZN respondents on the user acceptance of the systems.

8.8 Discussion

Bazeley (2009) highlights the absence of a guide on analysing and integrating qualitative and quantitative data. Ostlund et al. (2010) attempted to provide a guide by doing a methodological review of studies which used mixed methods. Using Erzberger and Kelle's (2003) triangulation diagram, they presented a scenario which led to four categories of triangle. One was convergent, which means the outcomes of qualitative and quantitative yielded the same conclusion. The second one was complementary, which means the results of quantitative and qualitative data could be utilised to supplement one another. The third was divergent, which means that the qualitative and quantitative results yielded different perspectives. The fourth scenario was the development of a theory, which means the results of the qualitative and quantitative brought new knowledge which forms the starting point for building a theory on how constructs are related.

All of these scenarios have been applied to this study. The aim of applying all the scenarios was to show the strength of utilizing both qualitative and quantitative data when using a mixed methods approach in a study. The first scenario triangulated complementary results in that the responses to both the quantitative and qualitative questions reaffirmed the other.

The second scenario on triangulated convergent results,–as demonstrated by the similarities in the concluding data for both qualitative and quantitative analysis. However, the findings did not convincingly support the theory of convergent results? It can therefore be concluded that this specific scenario does not strongly argue for the hypothesis of the study

The third scenario on triangulated divergent results, presenting an opposing outcome between the quantitative and qualitative results. However, it should be noted that there were a limited number of respondents who in the open-ended questions, expressed frustrations about the Innerweb system out of the 131 survey participants, 15 responded to the open ended questions of the third scenario, however not all of these presented negative views about the system). Therefore, this leaves the divergent results between qualitative data and quantitative data inconclusive.

The results gathered from the fourth scenario not only supplied a correlation between the qualitative and quantitative surveys but also provided a new set of information from the qualitative data that has the potential of becoming a new theory for the whole study.

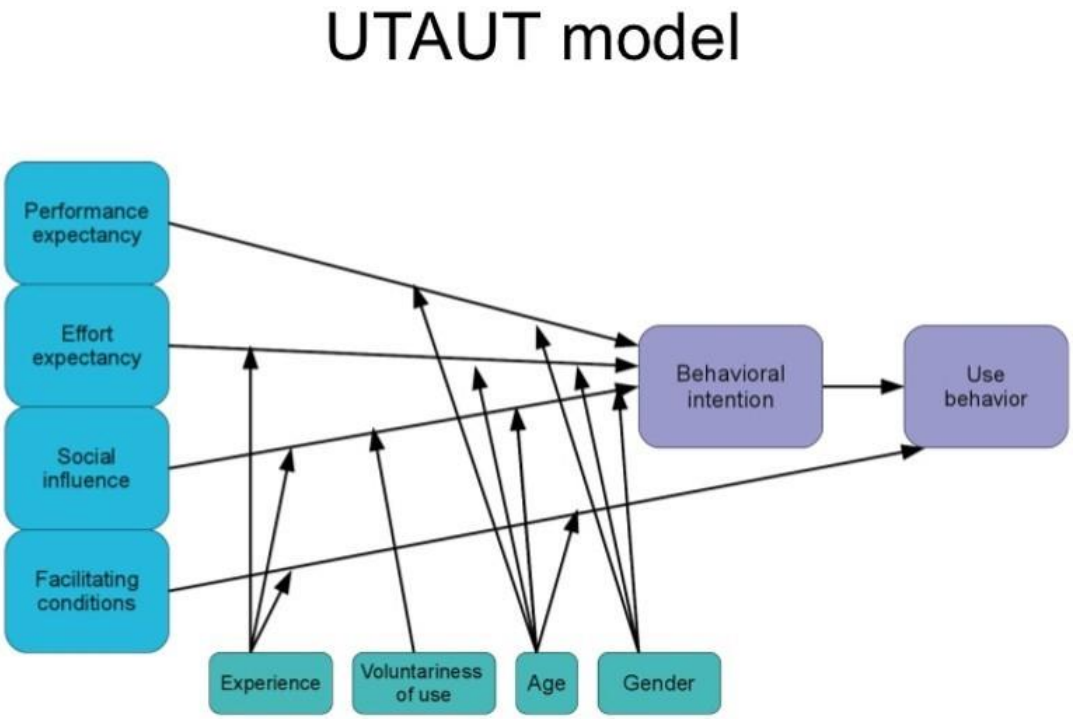


Figure 8.6: Illustration of UTAUT model (Alzubaidi, 2011).

The qualitative data results complemented the quantitative data results by confirming that respondents are using the systems positively and expressed how they could be improved. The quantitative findings on "to what extent do various factors influence user acceptance of information security systems methods for securing and archiving information at UKZN" led to conclusions that there is a strong positive correlation between performance expectancy and Behavioural Intention to Use the system. In other words, the agreement that the system will assist performance is correlated with agreement that they intend to use the system. Analysis reveals that there is a positive correlation between effort expectancy and behavioural intention to use the system. This therefore confirms that there is an agreement that effort expectancy will assist the behaviour agreement to use the system. In the relationship between social influence and behavioural intention to use the system, there is a positive strong correlation. It is therefore concluded that social influence plays a positive role in the behavioural intention to use the system. There is a strong positive correlation between facilitating conditions and behavioural intention to use the system. Therefore, the facilitating conditions contribute positively to a behavioural intention to use the system. Figure 8.6 above confirms these findings as it points to how the performance expectancy, effort expectancy and social influence lead to behavioural intention which further leads to use behaviour. Facilitating conditions also lead to use behaviour, with moderating factors like experience, age and gender being interlinked.

These results complement the qualitative results on the question "to what extent does the current system used to archive academic certificates at UKZN display problems related to employee perceptions of the university's information systems security measures". The results revealed that the organization supports the use of the system, which in turn supported the quantitative survey results. Further to that, the qualitative interviews revealed that an automated system was needed for the academic certificates and that the degree flow processes in place at UKZN do not include the archiving of degree certificates. However, the interviews did reveal the need for a repository, for three reasons: first, to act as a verification tool as part of the university's governance model at the university, through robust record keeping; second, to place the credibility and integrity of degrees in high esteem, and third, to provide assurance to oversight structures at UKZN, such as the Audit and Risk Committee and Council, that the degree certificates remain authentic and highly respected. A further recommendation was that the repository stores the graduation brochure or roll as a further measure of authentication of degree certificates.

The recommendations that came from the qualitative results is taken as new knowledge that could lead to an application of existing theory and a practical solution.

8.9 Knowledge contribution

Technology advances necessitate for organisations to continue to search for better ways of keeping important data highly secured. This study used the mixed methods approach for reliability of the results and the triangulating complementary results concluded that employees at UKZN are familiar with the systems for securing important data. Therefore, it could be concluded that employees' knowledge about the system in a workplace does not impose security threats. The results further reveal that the features and the system itself should be improving in order to secure and archive data. The qualitative study further revealed that the participants had suggested additional features they thought could enhance the security of academic certificates. The participants indicated that an automated system could be a good option. The trial implementation of how steganographic system works serves to address these gaps in the securing and archiving of academic certificates at UKZN. The study added new knowledge that while many studies argue that human intervention is known to compromise security in organisations, the results revealed that what will improve security of sensitive data in an organisation is the improvement of the system to have capabilities of blocking unauthorised users.

Therefore, this study closes the gap which Siponen and Baskerville (2018) identified that information system security management is one area which shows a substantial gap between theories used and practical intervention, which is witnessed by daily reports of information systems security and privacy breaches. The UTAUT theory was largely confirmed by the quantitative results. The new knowledge that was identified was that the system needs improvement in order to better secure and archive academic certificates and that human factors are not critical aspects, as is traditionally believed.

8.10 Conclusion

This chapter discussed in detail the results and used qualitative and quantitative results to establish the unique. The qualitative findings have been weighed against the quantitative results to identify complementary and divergent aspects. The chapter presented scenarios of how the results could be interpreted and how they shaped the study. The new knowledge which came from the qualitative study hinted a need for a practical automated system for archiving and securing the academic certificates. The next chapter demonstrates the process of embedding an image in another image and a certificate in an image, using the author's personal document and image. This implementation process could be viewed as a practical solution to enhancing the archiving and securing academic certificates at UKZN.

CHAPTER 9

THE PRACTICAL APPLICATION

9.1 Introduction

What emanates from the study is that the quantitative survey results revealed that there is a positive perception from the UKZN employees about using the system to archive and secure sensitive data. The qualitative data revealed that though there is a system in place which is currently used to secure academic certificates, it does not archive the academic certificates. Furthermore, the results revealed that there has been evidence of tampering with the academic certificates. A strong motivation was for print certificates that have more security features and for all the certificates to be automated. The qualitative results revealed that there is a need for an automated system to archive and secure academic certificates.

The literature review discussed the benefits of digitization and further highlighted the advantages of combining the digitization with security for maximum benefits of the documents archiving and security. The literature further expanded on looking at the type of security which is still considered to be strong and used by sensitive places like bank notes, home affairs and certificates. The literature highlighted that this type of security still carries maximum strength. Therefore, this chapter demonstrates how the combination of digitization and security, in particular cryptology, could be used in archiving and securing sensitive documents. The researcher's private documents will be used in this demonstration.

9.2 Trial implementation of steganographic system at UKZN

The interview questions were drafted to help establish the trial implementation of the steganographic system. The ICS and Records and Examination candidates were chosen for the trial implementation. The reason for choosing them is because it is convenient. The ICS candidate was chosen because he will be dealing with the technicalities of the system. The Records and examination candidate was chosen because the system for archiving and securing academic certificates resides in her department.

Participants: ICS and Examination and Records Department

9.2.1 Demonstrate the process you follow in running the system

The participant answered that installing the software was straightforward; *I ran the setup file and followed the prompt. When I launched the application, it prompted me for the file to encrypt and the image to embed, and then it generated an encrypted file and the decryption key*.

9.2.2 Integration of the steganographic system to other University systems

The participant answered that *The system is a standalone system, and it does not have any capabilities of harvesting data from other systems or pushing data to other systems. Human interaction will be required if it were to work with other systems*

9.2.3 Training End-Users

The participant revealed that *The system is very intuitive; any person who can use a computer will be able to navigate the system without any assistance*. This could be because the participant is qualified in information technology which makes it easy for him to use it.

9.2.4 Advantages and disadvantages of this new system

According to the participant *the advantage is that it is very simple to use product that can help the universities to encrypt the confidential document. The disadvantage is that there is no clear process of storing the decryption key, this means that if you accidentally lose the key, you will never be able to decrypt the file.*

9.2.4 System use

The ICS participant demonstrated the use of the system in order to show the Examination and Records Department participant. The ICS participant mentioned that this part of presentation will be the training for staff in the future if the system is adopted. The ICS participant used the author's documents during demonstration. The author's private certificates and photos were used because of the ethical clearance declaration which stated that only the author's private data will be used at this stage. (Appendix G):-

I am going to create a flow of how the system flow looks like in my demonstration. In my computer I have a scanner opened. I then scan the author's certificate which once scanned I saved it giving it a name, and this time I save it twice, one as a jpeg file and another one as a tiff file on a file folder I created called input_archive. I now upload the author's picture which

is a jpeg and safe it on the file folder called input_archive, I saved it with a name called embedder image. Now I launch the steganographic system, it prompts me immediately to upload first the file to be encrypted, which I upload from input_archive which is jpeg. As soon as the file is finished uploading it then prompt me to now upload the file to be embedded on, I then fetch the image on the input_archive and upload. As soon as the upload is finished, the system prompt itself to perform the encryption process which takes few minutes. The encrypted file is then generated which is an image where the file to be encrypted was embedded on. The image looks a bit different from the original image. Finally, the pin with eight numbers is generated and displayed on the system. To open the encrypted file the system only prompted me to put the pin that was generated.

The process of encrypting the certificates to photographs

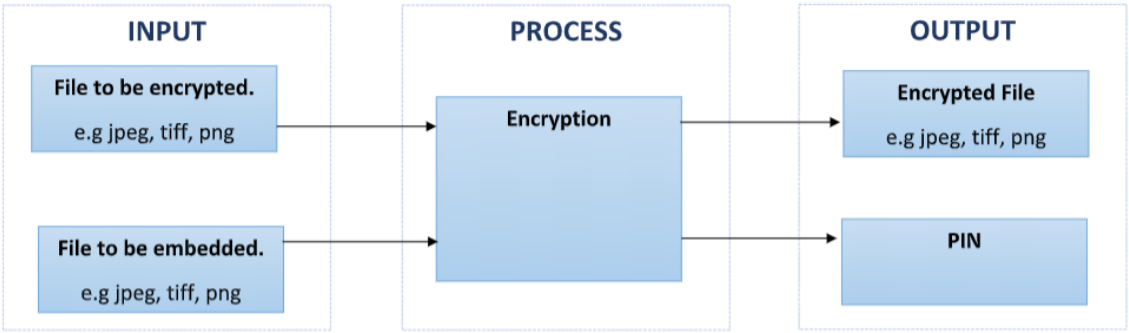


Figure 9.1 Encrypting process

9.2.5 The end-user experience of the system after demonstration

The end-user participant from the Examination and Records department was present when the ICS participant was demonstrating the system and was asked to comment about how she found the system demonstration and to define it in her own observation. *The process is simple and straightforward, everything is on a single screen, and the system is fast. At the beginning, it is not clear what the buttons E and D do, until someone tells you. This makes the system not fully intuitive; it would improve the usability of the system if names of the buttons were written in full.*

9.3 The software system discussion

The stegocrypt is a software system created to be used as a process of embedding documents in other documents. One feature of the software system is the input icon: this icon works with a browser button and is meant to identify the document which has to be embedded or protected. The browser harvests the document from any drive that the computer may have. The output

button which consists of its own browser button is meant to deliver the outcome when the document has been embedded into another document or an image. The host image which comes with its own browse button which is below the input button, is the button which could be utilised to fetch the image where the document to be protected with be embedded at. The pin button is a pin which gets generated to be used when the decryption of a document from the image is done. The execution below will outline the step by step process of how the program works.

9.3.1 Execution

Locate **StegoCrypt** in the **All Programs** menu and click **StegoCrypt** icon.

Figure 9.2: StegoCrypt System

The path for input file is a box that is utilized to fetch the image or plaintext that will be encrypted. The format of the document could be in jpeg, tiff, bmp and png. The path for output file is a box that is utilized to fetch the image that will be used to cover another image and is called covertext. This image or document could also be of any format. The path for output file is a box that is utilized to generate the document or image that is as a result of an application of covering image or document behind another image or document and is called stegotext. This image or document could be in any format. The pin box is where the pin gets generated after the action of hiding image in another image has taken place. It is an important pin that could be used to open a hidden image.

Figure 9. 3: Example of the application of function Encrypt: Plaintext image (left) I_1, Covertext image (middle) I_2, Stegotext .tiff image (right) I_3.

In Figure 9.2, the plaintext academic certificate document on the left is hidden in the image in the middle, which is a covertext image. The image on the right has a hidden certificate embedded in it. Looking at the pictures in the middle and right, it is difficult to see any difference unless you are aware that the right image has an embedded academic certificate.

Figure 9. 4: Example of the application of function Decrypt: Stegotext image (left) I_3, Covertext image (middle) I_2 and decrypt (right) I_4.

In Figure 9.3, the process of removing the academic certificate which was hidden in the image has taken place. The image on left had the academic certificate embedded in it. The image in the middle was used to cover the academic certificate and the academic certificate on the left was hidden behind the image on the left.

Figure 9.5: Example of the application of function Encrypt for self-authentication of a certificate: Plaintext image (left) I_1, Covertext image (middle) I_2, Stegotext.tiff image (right) I_3.

In Figure 9.4, the process of hiding plain text on the left with another plaintext in the middle has produced an image on the right which also is a plaintext image. It is very hard to identify the difference in the three plaintext images. This serves the purpose of ensuring that the document is archived and secured, but that it does not raise suspicions to those who are being deceived.

Figure 9.6: Example of the application of function Decrypt for the self- authentication of a certificate: Stegotext image (left) I_3, Covertext image (middle) I2and Decrypt image (right) I_4.

Figure 9.5 shows the process of removing the academic certificate which was hidden behind another academic certificate. It is extremely difficult to notice the changes in all the three documents. This ensures that the steganographic technology does protect without damaging the documents.

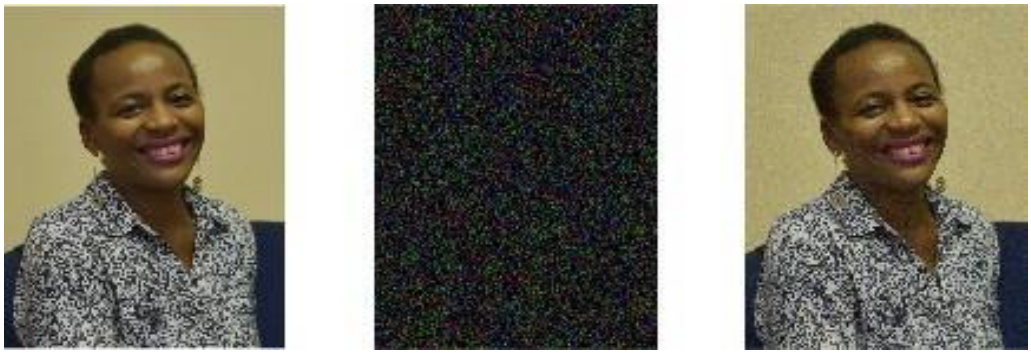


Figure 9.7: Example of the application of function POE and POD: Plaintext image (left) I1, Ciphertext image I2 (middle) - Equation (6.3), Decrypted image I1 (right) - Equation (6.4). check

Figure 9.6 shows the process whereby the image on the left undergoes a process of being hidden into another image. The image in the middle shows how the process takes place. The image on the right is the end product of the hidden image. If one looks closely, the image on the left looks smooth and clear while the image on the right is not as clear and smooth as the one on the left. This indicates that when you pay careful attention, there is a slight difference in images noted.

The next figure displays how the new version of the system will constitute an improvement on the old version as it includes image diffusion (improving security) and gives an exact (within small numerical error) decryption for full colour images.

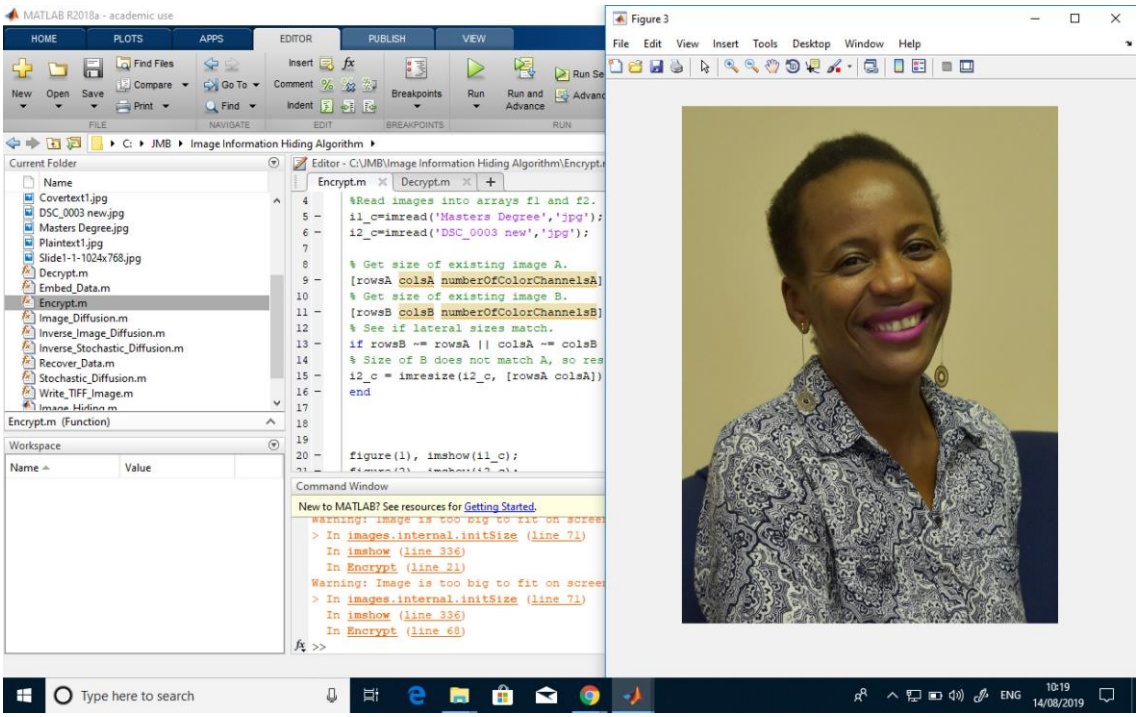


Figure 9.8: Example of the application of function POE and POD: Plaintext image (left) I1, Ciphertext image I2 (middle) - Equation (6.3), Decrypted image I1 (right) - Equation (6.4). check

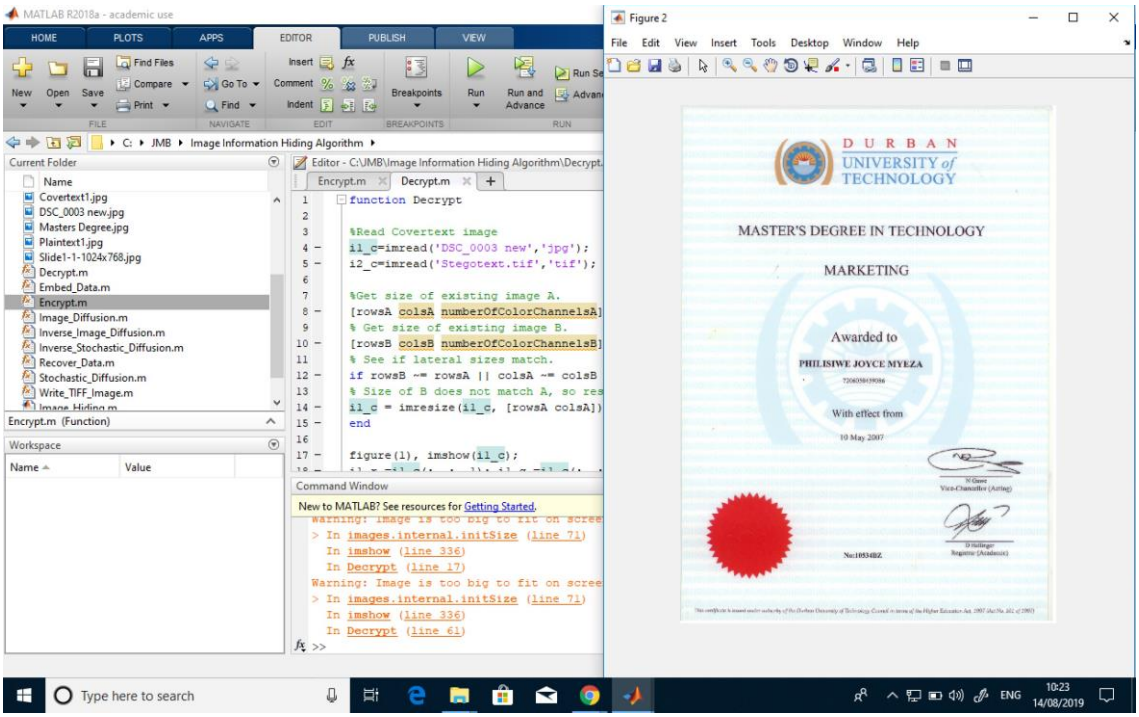


Figure 9.9: Example of the application of function POE and POD: Plaintext image (left) I1, Ciphertext image I2 (middle) - Equation (6.3), Decrypted image I1 (right) - Equation (6.4). check

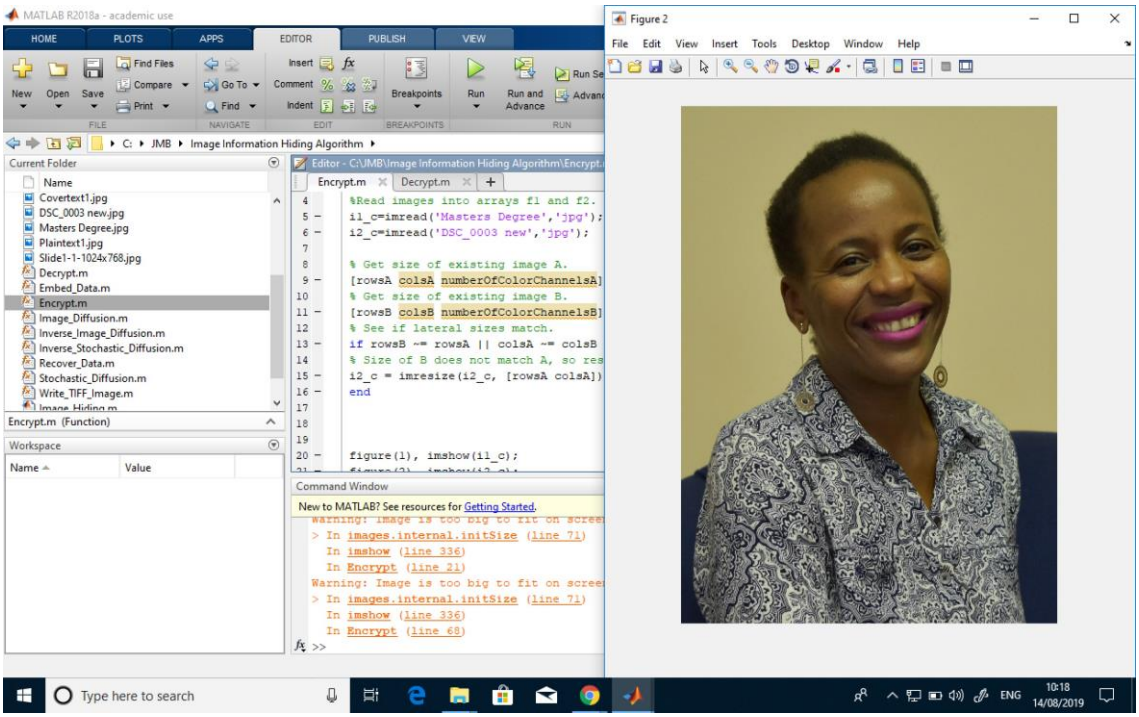


Figure 9.10: Example of the application of function POE and POD: Plaintext image (left) I1, Ciphertext image I2 (middle) - Equation (6.3), Decrypted image I1 (right) - Equation (6.4). check

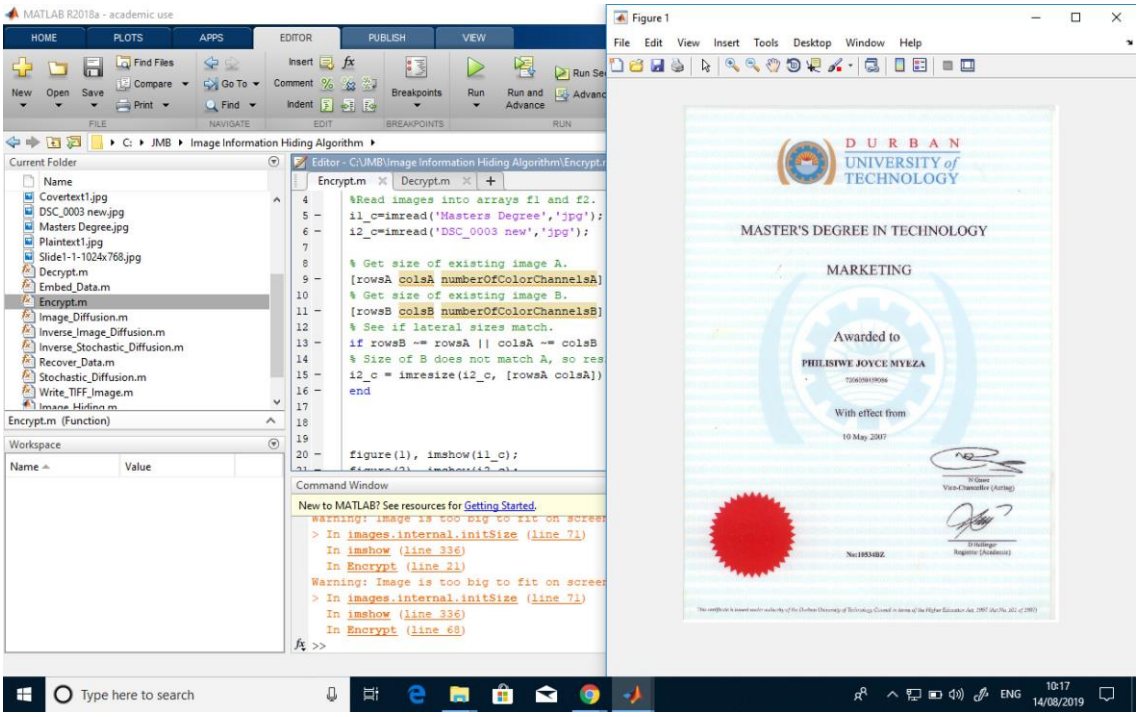


Figure 9.11: Example of the application of function POE and POD: Plaintext image (left) I1, Ciphertext image I2 (middle) - Equation (6.3), Decrypted image I1 (right) - Equation (6.4). check

9.4 Summary

This chapter discussed the demonstration of an implementation phase of steganographic system at UKZN. The two participants were selected to show how the system works and to run the system. The whole process demonstrated how an image can be hidden behind another image. The author's private documents were used to demonstrate how this method could function to improve security. A detailed technical discussion of how the software functions is found in Appendix B, and the programming scripts are in Appendices C, D, and E. The next chapter discusses the findings and the recommendations which emanate from this study.

CHAPTER 10

CONCLUSION

10.1 Introduction

This chapter presents the summary and conclusion of the research study. An overview of the key findings is provided, and the major implications and limitations of the study are described. Finally, recommendations for future research are offered.

10.2 Overview of Significant Findings

The objective of this study was to investigate the factors that affect employee acceptance of information systems security measures by using UTAUT to explore such acceptance in the specific case of UKZN. In addition, the study sought to examine issues around the securing and archiving of academic degree certificates. The UTAUT model was chosen as the theoretical framework because it best suited the context of information systems security at UKZN. The research incorporated an empirical study through the development of a survey questionnaire and interviews to study the influence of user acceptance of information security systems methods on the securing and archiving of information at UKZN. The intention was to study:

- how others' beliefs about information systems security affect UKZN employee perceptions of and intentions to use information systems security measures;
- how employees' perceptions affect their intentions to access information regarding the information systems security measures at UKZN, and
- to what extent does the current system used to archive academic certificates at UKZN has problems related to employee perceptions of information systems security measures at UKZN.

The specific research questions that were addressed are presented next with findings.

10.2.1 Research Question 1:

- To what extent do various factors influence user acceptance of information security systems methods in securing and archiving information at UKZN?
- The survey results reflected that various factors, such as performance expectancy, effort expectancy, and social influence, have a positive influence on the user acceptance of information security systems at UKZN.

10.2.1.1 The qualitative findings

The qualitative findings supported the quantitative data findings by eliciting responses from users who were familiar with the systems for securing and archiving academic certificates, and were using the systems positively, with full knowledge of the ITS and SMS systems.

10.2.1.2 The quantitative findings

- The majority of responses on performance expectancy for the respondents on using the Innerweb at UKZN strongly agreed on the chances of improving performance in operations, being useful, and increasing productivity, as well as helping with quicker accomplishment of tasks.
- of effort expectancy for the respondents on using the Innerweb at UKZN. The majority of responses agreed that it would be easy to be skilled, and to understand and learn how to operate the Innerweb.
- of social influence for the respondents on using the Innerweb at UKZN. The majority of responses agreed that the organization has supported the use of the Innerweb.
- of facilitating conditions for the respondents on using the Innerweb at UKZN. The majority of responses agreed that they have resources and knowledge necessary to use the Innerweb. They have found the Innerweb to be compatible with other systems, and at times when there were difficulties, assistance was available.

10.2.2 Research Question 2:

To what extent do employee perceptions regarding the information systems security measures at UKZN affect their intention to use information systems security measures?

- The analysis and results given in Chapter 6 show that the majority of respondents think that archiving and securing information is part of their job and that the majority of the respondents were familiar with the Innerweb system.

10.2.2.1 The qualitative findings

The qualitative results supported the quantitative surveys, with respondents who felt that securing and archiving academic certificates was part of their responsibilities. The respondents further revealed what they felt needed to be improved in the system so as to strengthen it.

10.2.2.2 The quantitative findings

The respondents responded positively on having knowledge about the Innerweb system at UKZN.

The majority of responses agreed that the organization has supported the use of the Innerweb.

10.2.3 Research Question 3:

To what extent do others' beliefs about the use of information systems security measures affect UKZN employees' perceptions of and intentions to use information systems security measures?

The results of Chapter 6 show that the majority of responses agreed that the organization has supported the use of Innerweb system and that there is always assistance available when there are systems difficulties. The majority of the respondents also agreed that they have the good intention, resources and knowledge necessary to use the Innerweb.

10.2.3.1 The qualitative findings

The qualitative results supported the quantitative survey, with respondents who were involved with the systems and aware of the weaknesses for the systems and contributed to how the system could be improved.

10.2.3.2 The quantitative findings

The responses reflected that people who are important to respondents were helpful with respect to the use of the Innerweb system. The majority of responses agreed that the organization has supported the use of the Innerweb.

The majority of respondents agreed that the Innerweb system was compatible with other systems they use. The majority of responses agreed that they have resources and knowledge necessary to use the Innerweb. They have found the Innerweb to be compatible with other systems, and at times when there were difficulties, assistance was available.

10.2.4 Research Question 4:

To what extent does the current system used to archive academic certificates at UKZN have problems related to employee perceptions of information systems security measures at UKZN?

10.2.4.1 The qualitative findings

The qualitative results supported the quantitative survey, with respondents who felt that securing and archiving academic certificates was part of their responsibilities. The respondents further revealed what they felt needed to be improved in the system so as to strengthen it.

The qualitative interviews revealed that the degree flow processes in place at UKZN do not include the archiving of degree certificates and there is an urgent need for an automated system with good security software. However, the interviews did reveal the need for a repository, for three reasons: first, to act as a verification tool as part of the university's governance model at

the university, through robust record keeping; second, to place the credibility and integrity of degrees in high esteem, and third, to provide assurance to our oversight structures at UKZN, such as the Audit and Risk Committee and Council, that the degree certificates remain authentic and highly respected. A further recommendation was that the repository stores the graduation brochure or roll as a further measure of authentication of degree certificates. The survey revealed that the majority of participants felt that archiving and securing information at the University was part of the job they performed every day. Furthermore, the interviews revealed that the university's certificates have been compromised by outsiders, which has led to the university needing to place additional safety features on the hard-copy certificate.

10.2.4.2 The quantitative findings

The quantitative survey revealed a strong positive correlation between performance expectancy, effort expectancy, social influence, facilitating conditions and behavioural intention to use the system. The quantitative findings supported the qualitative results by revealing that there is positive correlation between performance expectancy, effort expectancy, social influence and behavioural intention to use the system.

The study used both qualitative and quantitative data, while the results confirmed Davis's theory but what is important is these results led to a practical testing of the theory. This brings a new meaning to the existing theory and closes the gap that has been existing in information systems security where theory does not seem to be providing practical solutions. The novelty in this study is that the results, though they were tested in the UKZN context, could be adapted to other entities with similar challenges.

10.3 Implications of the Study

Siponen and Baskerville (2018) state that the results of the current Information Systems Security research in practice, is that it does not indicate the best approach to practitioners or highlight which of these empirically tested theories are the most effective for solving ISS problems.

This study was built around four research questions. It set the scene for University Executives and information security managers to consider the steganographic method system with regard to strengthening security further and could be used in the future to develop a stegano-technographic system for sensitive data.

10.4 Limitations of the Study

There were limitations to this study. The collection of data was carried out at a time when the university was undergoing serious fraud investigations; consequently, many staff members were overly cautious and did not want to engage in surveys. This had a negative effect on the number of responses received. Another limitation was the use of the university's own software to administer the survey: because the questions were about current software, there might have been limited objectivity in response to questions about the university's information systems in general. The limitation was managed by having open-ended questions and using qualitative analysis to triangulate with the quantitative data. There was also the limitation of UTAUT as a framework for the study, as the qualitative analysis identified an additional construct that could be added to the UTAUT framework.

10.5 Contribution to the body of knowledge

Oates (2006) defines the outcomes of research, especially the contribution to knowledge in a thesis, as a contribution that can be "an answer to the original research question(s) but can also include unexpected findings" (Oates 2006, p.11). Moreover, she suggests various types of different knowledge outcomes: a new or improved product, a new theory, a re-interpretation of an existing theory, a new or improved research tool or technique, a new or improved model or perspective, an in-depth study of a particular situation, or an exploration of a topic, area or field or a critical analysis. This study is an in-depth study of user acceptance of steganographic methods in securing digital certificates at the University of KwaZulu-Natal and has clearly answered the research questions posed.

Furthermore, Agertalk (2014) argues that it is sometimes more useful to make a sound contribution to practice rather than a vague theoretical contribution.

The literature shows that there is widespread fraud in electronic documents and further confirms various methods that have been used to curb such fraudulent manipulation. One of the existing methods is hiding data behind data, which is called steganography. However, the literature does not reveal any use of this method in archiving electronic documents as a form of preventing the fraudulent activities.

Therefore, the significance of the study is in drawing attention to the use of steganographic methods in securing and archiving documents and the practical demonstration of the use of steganography methods in archiving academic certificates.

The findings presented provide insight into the possible use of steganographic methods in the higher education sector, specifically in the archiving of academic certificates. The practical application of steganographic methods to digital archiving serves as one instance of other possible applications of securing digital documents, both in the higher education sector and beyond.

10.6 Conclusion and Recommendations for Future Studies

The use of the unified theory of acceptance and use of technology led to the conclusion in this study that performance expectancy, effort expectancy and social influence had a significant positive impact on behavioural intentions of the acceptance of information security measures at UKZN. Behavioural intention and facilitating conditions had a direct effect on usage. Print and electronic documents, as well as the latest technological developments, are a target for fraudulent activities. One way to secure confidential documents in a digital library against these activities, is to hide data within other data in a digital library. A method for decrypting hidden data to establish the authenticity and originality of a document, will be useful in helping with the authenticated verification process.

Future research should focus mainly on testing and implementation of the steganographic methods on important data, especially degree certificates and challenging computer science students to try to break the encryption.

In addition, future research should review the function of steganography in a digital library. The software listed in Appendices B to D detail the process of securing data using the steganotechnographic method considered in this work.

The steganotechnographic system is one of the few technologies which have been known to discourage unwanted intruders. However, this study did not investigate other similar technologies which may be utilised to secure and archive sensitive data. Future studies need to explore these alternative technologies comparatively and to compare and identify stronger systems for securing sensitive data.

BIBLIOGRAPHY

Abadia, C.E., Oviedo, D.G., 2009. Bureaucratic itineraries in Colombia. A theoretical and methodological tool to assess managed-care health care systems. Social Science & Medicine 68 (6), 1153–1160.

Adekanmbi, O. and Green, P. 2015. "Assessment of User Authentication Risks in a Healthcare Knowledge Management System", *International Business and Economics Research Journal*, Vol. 14, No. 1. Accessed on 17 January, 2016 at www.library.ukzn.ac.za

Adesina, A. et. al. 2011. "Ensuring the Security and Privacy of Information in Mobile Healthcare Communication Systems, *South African Journal of Science*, Vol. 107, No. 9. Accessed on 16 January, 2017 at www.library.ukzn.ac.za

"Advanced Secure Technologies", 2016. Accessed on June 06, 2017 at www. advancedsecure.co.uk

Agrawal, N. and Savvides, M. 2009. "Biometric Data Hiding: A3 Factor Authentication Approach to Verify Identity with a Single Image using Steganography, Encryption and Matching"', Pittsburgh, PA: Carnegie Mellon University. Accessed January 24, 2016 at www.library.ukzn.ac.za

Ajzen, I. 2013. "From Intentions to Actions: A Theory of Planned Behavior", 1985, in Wong, K., et. al., "Understanding Student Teachers' Behavioural Intention to use Technology: Technology Acceptance Model (TAM) Validation and Testing"', *International Journal of Instruction*, Vol. 6,
No. 1. Accessed January 17, 2016 at www.library.ukzn.ac.za

Ajzen, I. and Fishbein, M. 1980. "Understanding Attitudes and Predicting Social Behavior", 1980, in Wong, K., et. al., "Understanding Student Teachers' Be- havioural Intention to use Technology: Technology Acceptance Model (TAM) Validation and Testing"', *International Journal of Instruction*, Vol. 6, No. 1. Acccessed January 17, 2016 at www.library.ukzn.ac.za

Aktas, H. and Kalkan, M. 2014. "An Application of Crystography", *Journal of Mathematics and Computer Science*, Vol. 11. Accessed 9 February, 2016 at www.library.ukzn.ac.za

Alfreds, D.n2014. "Ex-cop Received Fake Matric Certificate from Teacher", *South African online News24*. Accessed 23 October, 2016 at www.news24.co. za

Al-Rawi, A. 2014. “A Study of Steganocryptography with Applications to Image and Audio Data”, PhD Thesis, Dublin Institute of Technology. Accessed January 02, 2016 at www.library.ukzn.ac.za

Alzubaidi, A. 2011. UTAUT model diagram. Technology Acceptance – useful links. Accessed June 03, 2019 at https://ausalzubaidi.wordpress.com/author/ausalzubaidi/

Atawneh, S. et al. 2013. “Steganography in Digital Images: Common Approaches and Tools”, *IETE Technical Review*, Vol. 30, No. 4, 2013. Accessed January 02, 2016 at www.library.ukzn.ac.za

Avison, D. Gregor, S, and Wilson, D. 2006. Managerial IT unconsciousness, communications of the ACM, Vol. 49, No. 7, pp. 88-93.

Babbie, E. 1990. *Survey Research Methods*, Wadsworth: Wadsworth Publishers.

Bacharach, S. 1989. Organizational theories: some criteria for evaluation, Academy of Management Review, Vol. 14, No. 4, pp. 496-515.

Baskerville, R. 2008. “What Design Science is Not”, *European Journal of Information Systems*, Vol. 17, pp. 441-443. Accessed January 02, 2016 at www.library.ukzn.ac.za

Bazeley, P., 2009. Analysing mixed methods data. In: Andrew, S., Hal- comb, E.J. (Eds.), Mixed Methods Research for Nursing and the Health Sciences. Wiley-Blackwell, Chichester, pp. 84 118.

Beatty, P.W., Neri, M.T., Bell, K., DeJong, G., 2004. Use of outcomes information in acute inpatient rehabilitation. American Journal of Physical Medicine & Rehabilitation 83 (6), 468 478.

Bernardi, L., Kleim, S., von der Lippe, H., 2007. Social influences on fertility: a comparative mixed methods study in Eastern and Western Germany. Journal of Mixed Methods Research 1 (1), 23–47.

Bertino, E. and Sandhu, R. 2005. “Database Security: Concepts, Approaches and Challenges”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 2, No. 1. Accessed 17 February, 2016 at www.library.ukzn.ac.za

hasker, R. 1989. *Reclaiming Reality: A Critical Introduction to Contemporary Philosophy*, London, Verso.

Blackledge, J. M. and Coyle, E. D. 2009. “Information Hiding by Stochastic Diffusion and its Application to Printed Document Authentication”, *Proc. of IET ISSC2009*, UCD (June 10-11, 2009), Vol. 20, No. 1, PS-4, pp. 1-6.

Blackledge, J. M., Bezobrazov, S., Tobin, P. and Zamora, F. 2013. "Cryptography using Evolutionary Computing", *Proc. IET ISSC2013*, Letterkenny, Co Donegal, Ireland, June 20-21.

Blackledge, J. M., Tobin, P. and Bezobrazov, S. 2015. "Cryptography using Artificial Intelligence", *The International Joint Conference on Neural Networks* (IJCNN2015), Killarney, Ireland, 12-17 July, 2015.

Blackledge, J. M. 2010. "Information Hiding using Stochastic Diffusion for the Covert Transmission of Encrypted Images", *Proc. of IET ISSC2010* UCC Cork, 23-24 June.

Blackledge, J. M. and Coyle, E. 2010. "e-Fraud Prevention Based on the Self- Authentication of e-Documents", *IEEE, Digital World 2010 First International Conference on Technical and Legal Aspects of the e-Society*, 2010. Ac- cessed January 16, 2016 at:
http://arrow.dit.ie/engscheleart/150/

Blackledge, J. M. and Al-Rawi, A. R. 2011. "Steganography using Stochastic Diffusion for the Covert Communication of Digital Images", *IANEG International Journal of Applied Mathematics*, Vol. 41, Issue 4, pp. 270-298.

Blackledge, J. M. and Dubovitskiy, A. 2011. "A Covert Encryption Method for Applications in Electronic Data Interchange". Accessed on 16 January, 2016 at www.library.ukzn.ac.za

Blackledge, J. M. 2012. *Cryptography using Steganography: New Algorithms and Applications*, CAS Textbooks, Centre for Advanced Studies, Warsaw University of Technology, Poland, ISBN: 978-83-61993-05-6. Accessed on 02 January, 2016 at http://arrow.dit.ie/engscheleart2/40/

Blackledge, J. M. and Al-Rawi, A. R. 2013. "Image Authentication using Stochas- tic Diffusion", *Systems Informatics: Modelling and Simulation*, UKSIM2013, 10-12 April, Cambridge University.

Blackledge, J. M., Tobin, P., Myeza, J. and Adolfo, C. M. 2017. "Information Hiding with DataDiffusion using Convolutional Encoding for Superencryption", *International Journal for Pure and Applied Mathematics (Mathematica Aeterna)*, Vol. 7, No. 4, 319-356.

Blackledge, J. M., Govere, W. and Sibanda, D., "Phase-Only Digital Encryption", IAENG International Journal of Applied Mathematics, To be published, 2019.

Blum, M. and Goldwasser, S. 1985. "An Efficient Probabilistic Public-key Encryption Scheme which Hides all Partial Information", *Advances in Cryptology*, Vol. 84.

Bogdan, R. and Biklen. 2003. *Qualitative Research for Education: An Introduction to Theory and Methods*, Edition 4, Boston: Allyn and Bacon. Accessed January 20, 2016 at www.library.ukzn.ac.za

Boock, M. 2008. “Perspectives on: Organizing for Digitization at Oregon State University: A Case Study and Comparison with ARL Libraries”, *The Journal of Academic Librarianship*, Vol. 34, No. 5, pp. 445-451. Accessed on 02 June, 2016 at www.google.scholar.com

Borgman, C. L. (1996), “Social Aspects of Digital Libraries”, in E.A. Fox & G. Marchionini (Eds.), *Proceedings of the 1st ACM International Conference on Digital Libraries*, pp. 170-171, Bethesda, MD. Accessed on 02 June 2016 at: www.google.scholar.com

Boucher, D. 2013. *An Information Privacy Model for Primary Health Care Facilities*, MSc Thesis, University of Fort Hare, 2013. Accessed January 16, 2017 at www.library.ukzn.ac.za

Brannen, J., 2009. Prologue: mixed methods for novice researchers: reflections and themes. International Journal of Multiple Research Approaches 3 (1), 8–12.

Briggs, C. 1986. *Learning How to Ask: A Sociolinguistic Appraisal of the Role of the Interview in Social Science Research*, Cambridge University Press, 1986.

Bryman, A., 2004. Social Research Methods. University Press, Oxford.

Bryman, A., 2006. Integrating quantitative and qualitative research: how is it done? Qualitative Research 6 (1), 97–113.

Bryman, A., 2007. Barriers to integrating quantitative and qualitative research. Journal of Mixed Methods Research 1 (1), 8–22.

Burstein, F. and Gregor, S. 1999. The systems development or engineering approach to research in information systems: an action research perspective, in proceedings of the 10th Australian conference on information systems, B. Hope and P. Yoong (eds), Victoria University of Wellington, New Zealand, pp. 122-134.

Bussing, R., Koro-Ljungberg, M.E., Gary, F., Mason, D.M., Garvan, C.W., 2005. Exploring help seeking for ADHD symptoms: a mixed-methods approach. Harvard Review of Psychiatry 13 (2), 85–101.

Canales, M.K., Rakowski, W., 2006. Development of a culturally specific instrument for mammography screening: an example with American Indian women in Vermont. Journal of Nursing Measurement 14 (2), 99–115.

Capra, F. 2002. *The Hidden Connections: A Science for Sustainable Living*, 2002, London: Flamingo.

Charmaz, K. 2008. “Grounded Theory as an Emergent Method”, in Hesse Biber, S. N. & Leavy, P. (Eds.) *Handbook of Emergent Methods*, pp. 155-70, Guilford Press.

Cheng, G.Y., 2004. A study of clinical questions posed by hospital clinicians. Journal of the Medical Library Association 92 (4), 445–458.

Chen-Wilson, L., Gravell, A. and Argles, D. 2011. *Giving You Back Control of Your Data Digital Signing Practical Issues and the e-Cert Solution*, University of Southampton, School of Electronic and Computer Science, Learning Societies Laboratory. Accessed January 18, 2016 at www.library.ukzn.ac.za

Cheong, S. et al. 2013. *Secure Encrypted Steganography Graphical Password Scheme for a Near Field Communication Smartphone Access Control System*, Malaysia: Faculty of Engineering, Multimedia University. Accessed January 16, 2016 at www.library.ukzn.ac.za

Che-Wei, L. and Wen-Hsiang, T. 2012. "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image with a Data Repair Capability", *IEEE Transactions on Image Processing*, Vol. 21, No. 1. Accessed on January 17, 2017 at www.library.ukzn.ac.za

Clarke, P.N., Yaros, P.S., 1988. Research blenders: commentary and response. Transitions to new methodologies in nursing sciences. Nursing Science Quarterly 1 (4), 147–151.

Cochrane, 2009. Cochrane Handbook for Systematic Reviews of Interventions. http://www.cochrane-handbook.org/. The Cochrane Collaboration.

Cornford, T. and Smithson, S. 1996. *Project Research in Information Systems: A Student's Guide*, Macmillan. Accessed on January 02, 2016 from www.library.ukzn.ac.za

Cox, I., Miller, M., Bloom, J. Fridrich, J. and Kalker, T., 2007. "Digital Watermarking and Steganography", Morgan-Kaufmann, (e-Book) ISBN: 9780080555805.

Coyle, K., 2006. "Managing Technology: Mass Digitization of Books", Journal of Academic Librarianship. Vol. 32, No. 6. pp. 641-645. Accessed on 02 June 2016 at www.sciencedirect.com

Crabtree, B. and Miller, W., 1992. *A Template Approach to Text Analysis: Developing and using Codebooks*, Doing Qualitative Research, Newbury Park, CA, Sage Publications. Creswell, J., 2007. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, Sage Publications. Accessed January 02, 2016, at: www.library.ukzn.ac.za

Creswell, J.W., 2003. Research Design: Qualitative, Quantitative and Mixed Methods Approaches. Sage, Thousand Oaks.

Creswell, J.W., Plano Clark, V.L., 2007. Designing and Conducting Mixed Methods Research. Sage, Thousand Oaks.

Cushing, B. 1990. Frameworks, paradigms and scientific research in management information systems, Journal of Information Systems, Vol. 4, No. 2, pp. 38-59.

Davis, F. 1986. A technology acceptance model for empirically testing new end-user information systems: theory and results, unpublished doctoral dissertation, Sloan school of management, Massachusetts Institute of Technology.

Davis, F. 1989. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology", *Management Information Systems Quarterly*, Vol. 13, No. 3. Accessed, January 17, 2016 at www.library.ukzn.ac.za

Davis, F., Bagozzi, R. and Warshaw, P. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", *Management Science*, Vol. 35, No. 8. Accessed January 17, 2016 at www.library.ukzn. ac.za

Davis, G. and Oslon, M. 1985. Management information systems: conceptual foundations, structure and development. (2nd ed.), McGraw-Hill, New York.

Deetz, S. 1996. "Describing Differences in Approaches to Organization Science: Rethinking Burrell and Morgan and their Legacy", *Organization Science*, Vol. 7, No. 2, pp. 191-207. Accessed January 10, 2016 at: www.library. ukzn.ac.za

De Jager, K. and Brown, C. 2010. "The Tangled Web: Investigating Academics' Views of Plagiarism at the University of Cape Town", *Studies in Higher Education*, Vol. 35, No.5. Accessed on 20 June, 2017 at www.library.ukzn. ac.za

Denzin, N. and Lincoln, Y. 2005. *The SAGE Handbook of Qualitative Research*, Edition 2, Thousand Oaks: Sage Publications.

DiMaggio, P. 1995. Comments on 'What theory is not administrative sciences Quarterly, Vol. 40, No. 3, pp. 391-397.

Di Zenise, M., Vitaletti, A. and Argles, D. 2011. *A User-centric Approach to e Certificatesfor Electronic Identities (eIDs) Management in a Mobile Environment*, 2011, Italy: University of Rome 'Sapienza'; United Kingdom: University of Southampton. Accessed January 05, 2016 at: www.library.ukzn.ac.za

Draycott, C. 2000. "The Wellcome Trust Medical Photographic Library Digitization Project: A Case Study", *Journal of Audiovisual Media in Medicine*, Vol. 23, No. 4., pp. 165-170. Accessed on 02, June 2016 at www.google.scholar.com

Du Plessis, L. et al. 2015. *Verification of Qualifications in Africa*, Vanderbijl park, South Africa:

North-West University, Vaal Triangle Campus. Accessed January 8, 2015 from: http://www.saqa.org.za/docs/genpubs/

2015/Verification%20of%20Qualifications%20in%20Africa.pdf Duntsch, I. and Orlowska, E.

2000. “Logics of Complementarity in Information Systems”, *Mathematical Logic Quarterly*, Vol. 46, No. 2. Accessed January 04, 2016 at www.library.ukzn.ac.za

Erzberger, C., Kelle, U., 2003. Making inferences in mixed methods: The rules of integration. In: Tashakkori, A., Teddlie, C. (Eds.), Handbook of Mixed Methods in Social & Behavioural Research. Sage, Thousand Oaks, pp. 457–488.

Faqih, K. 2013. “Exploring the Influence of Perceived Risk and Internet Self- efficacy on Consumer Online Shopping Intentions: Perspective of Technology Acceptance Model”, *International Management Review*, Vol. 9, No. 1, 2013. Accessed June 09, 2017 at www.library.ukzn.ac.za

Feng, X., & Behar-Horenstein, L. (2019). Maximizing NVivo Utilities to Analyze Open-Ended Responses. *The Qualitative Report*, *24*(3), 563-571. Retrieved from https://nsuworks.nova.edu/tqr/vol24/iss3/11

Fishbein, M. and Ajzen, I. 1975. “Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research”, in Wong, K. et al. (2013), Under- standing Student Teachers’ Behavioural Intention to use Technology: Technol- ogy Acceptance Model (TAM) Validation and Testing. *International Journal of Instruction*, Vol. 6, No. 1. Acccessed January 17, 2016 at www.library. ukzn.ac.za

Fleischhauer, C. 2003. “Electronic Information and Digitization: Preservation and Security Challenges”, Chapter 17: Preservation, Security and Digital Content, *Journal of library administration*, Vol. 38, No. 3. Accessed 09, February 2016 at www.library.ukzn.ac.za

Fordyce, S. 1982. *Computer Security: A Current Assessment*, North-Holland Publishing Company. Accessed 16 January 2016 at www.library.ukzn. ac.za

Foss, C., Ellefsen, B., 2002. The value of combining qualitative and quantitative approaches in nursing research by means of method triangulation. Journal of Advanced Nursing 40 (2), 242–48.

Frels, J., Frels, R. and Onwuegbuzie, A. 2011. “Geographic Information Systems: A Mixed Methods Spatial Approach in Business and Management Research and Beyond ”*International Journal of Multiple Research Approaches*, Vol. 5, No. 3. Accessed January 04, 2016 at ww.library.ukzn.ac.za

Genise, P. 2002. *Usability Evaluation: Methods and Techniques*. Ac- cessed June 28, 2016 at http://www.cs.utexas.edu/users/almstrum/ cs370/elvisino/usaEval.html

George, C. 2005. “Testing the Barriers to Digital Libraries: A Study Seeking Copyright Permission to Digitize Published Works”, *New Library World*, Vol. 106, No. 1214/1215, pp. 332-342. Accessed on 02, June 2016 at www. google.scholar.com

Gernetzky, K. 2015. *Finding Fake Qualifications a Thriving Business*, Business Day Live, 2015. Accessed June 24, 2016 from:

http://www.bdlive.co.za/national/education/2015/01/15/finding-fake-qualifications-a-thrivingbusiness

Giddens, A. 1984. The constitution of society, polity press, Cambridge, UK.

Goel. S. and Chen, V. 2008. "Can Business Process Re-engineering Lead to Security Vulnerabilities: Analyzing the Re-engineered Process", *International Journal Production Economics*, Vol. 115. pp. 104-112. Accessed on 02, June 2016 at www.elsevier.com/locate/ijpe

Goldwasser, S. and Micali, S. 1982. "Probabilistic Encryption and How to Play Mental Poker Keeping Secret all Partial Information", in Proceedings of the 14th STOC.

Goncalves, M. et al. 2007. "What is a Good Digital Library: A Quality Model for Digital Libraries", *Information Processing and Management*, Vol. 43. pp. 1416-1437. Accessed on 02 June 2016 at www.elsevier.com/locate/ infoproman

Goran, G. 2012. "Pragmatism vs. Interpretivism in Qualitative In- formation Systems Research", *European Journal of Information Systems*, Vol. 21, No. 2, pp. 135-146. Accessed March 10, 2016 at:http://dx.doi.org/10.1057/ejis.2011.54Copyright:PalgraveMacmillan http://www.palgrave-journals.com/pal/index.html

Gregor, S. 2006. "The Nature of Theory in Information Systems", MIS Quarterly, Vol. 30, No. 3, pp. 611-642.

Gregor, S. 2002. A theory of theories in information systems in information systems foundations: building the theoretical base, S Gregor and D Hart (eds), Australian National University, Canberra, pp. 1-20.

Grimmelmann, J. 2010. "D is for Digitize: An Introduction", Vol. 55. Accessed on 02, June 2016 at www.google.scholar.com

Guba, E. and Lincoln, Y. 1994. "Competing Paradigms in Qualitative Re- search", in Denzin, N. K. & Lincoln, Y. S., Handbook of Qualitative Research, Sage Publications.

Halcomb, E.J., Andrew, A., 2009a. Managing mixed methods projects. In: Andrew, S., Halcomb,

E.J. (Eds.), Mixed Methods Research for Nursing and the Health Sciences. Wiley-Blackwell, Chichester, pp. 50–64.

Halcomb, E.J., Andrew, A., Brannen, J., 2009b. Introduction to mixed methods research for nursing and the health sciences. In: Andrew, S., Halcomb, E.J. (Eds.), Mixed Methods Research for Nursing and the Health Sciences. Wiley-Blackwell, Chichester, pp. 3–12.

Halcomb, E.J., Davidson, P.M., Griffiths, R., Daly, J., 2008. Cardiovascular disease management: time to advance the practice nurse role? Australian Health Review 32 (1), 44–53.

Hallak J. and Poisson, M. 2007. *Higher Education in the World: Academic Fraud, Accreditation and Quality Assurance*, pp 109-123. Accessed January 16, 2016, at www.library.ukzn.ac.za

Hallot, M. 2008. *Digital Watermarking Methods for Data Security and Authentication*, PhD Thesis, Department of Computer Science, University of the West- ern Cape, Republic of South Africa (a thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy). Accessed January 20, 2016 at https://scholar.google.com

Hashim, J. 2008. "Factors Influencing the Acceptance of Web-based Training in Malaysia: Applying the Technology Acceptance Model", International Journal of Training and Development. Vol. 12, No. 4. Accessed on June 10, 2017 at www.library.ukzn.ac.za

Hevner, A. et al. 2004. "Design science in information systems research. MIS Quarterly", Vol. 28, No. 1, pp. 75-105. Accessed on March 10, 2016 at https://scholar.google.com

Hoffman, A. 2016. *A Pilot Implementation of Certificate Authentication based on Digital Signatures*, North-West University. Potchefstroom Campus, 2016. Accessed 10 August, 2017 at www.library.ukzn.ac.za

Hopper, N. 2004. *Toward a Theory of Steganography*, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA.

Hoxmeier, J. and Lenk, M. 2020. Service-Learning in information systems courses: Community projects that make a difference. Journal of Information Systems Education, Vol.14, No. 1, pp. 91-100. Accessed June 07, 2020 at https://aisel.aisnet.org/jise/vol14/issi/10

Hussey, J. and Hussey, R. 2012. *Business Research: A Practical Guide for Under- graduate and Postgraduate Students*, Basingstoke, England, Macmillan Press, 1997.

International Association of Universities (IAU). Accessed on April 17, 2016 from CHE website http://www.iau-aiu.net/content/ policy-statements-0

Im, I., Hong, S., and Kang, M. 2011. "An International Comparison of Technology Adoption Testing the UTAUT model", Information and Management. Vol. 48. Accessed on June 10, 2017 at www.library.ukzn.ac.za

Ineson, C. 2013. *Higher Education Degree Datacheck (HEDD): Forgers Tar- get Cash Strapped Student*s. Accessed March 18, 2016 at https://heddblog.wordpress.com/author/craigineson/

Jick, T.D., 1979. Mixing qualitative and quantitative methods: triangulation in action.

Administrative Science Quarterly 24, 602–611.

Johnson, R. and Onwuegbuzie, A. 2004. "Mixed Methods Research: A Research Paradigm whose Time has Come", *Educational Researcher*, Vol. 33, No. 7. Accessed January 16, 2017 at www.library.ukzn.ac.za

Jones, C. 2009. *Utilizing the Technology Acceptance Model to Assess Employee Adoption of Information Security Measures*, Doctorate of Business Administration, 2009, H. Wayne Huizenga School of Business and Entrepreneurship, Nova Southeastern University.

Jones, C. et al. 2010. "Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures", *Issues in Information Systems*, Vol. XI, No.1. Accessed June 10, 2017 at www. library.ukzn.ac.za

Juaneda-Ayenza, E., Mosquera, A, and Murillo, Y. 2016. "Omnichannel Customer Behavior: Key Drivers of Technology Acceptance and Use and their Effects on Purchase Intention", *Frontiers in*
Psychology, Vol. 7. Accessed June 09, 2017 at www.library.ukzn.ac.za

Johnson, R.B., Onquegbuzie, A.J., 2004. Mixed methods research: a paradigm whose time has come. Educational Researcher 33 (7), 14–26.

Kartalova-O'Doherty, Y., Tedstone Doherty, D., 2009. Satisfied carers of persons with enduring mental illness: who and why? The International Journal of Social Psychiatry 55 (3), 257–271.

Kelle, U., 2001. Sociological explanations between micro and macro and the integration of qualitative and quantitative methods. Forum: Qualitative Social Research 2 (1), 5 Art.

Khan, K.S., 2001. Undertaking Systematic Reviews of Research on Effectiveness: CRD's Guidance for those Carrying Out or Commissioning Reviews. Centre for Review and Dissemination, York.

Kroll, T., Neri, M., 2009. Designs for mixed methods research. In: Andrew, S., Halcomb, E.J. (Eds.), Mixed Methods Research for Nursing and the Health Sciences. Wiley-Blackwell, Chichester, pp. 31–49.

Kaplan, B., and Maxwell, J. 1994. "Qualitative Research Methods for Evaluating Computer Information Systems", in J. G. Anderson, C. E. Aydin & S. J. Jay (Eds.)
Evaluating Health Care Information Systems: Methods and Applications, pp. 45-68, Thousand Oaks, CA, Sage.

Kelle, U., Kuhberger, C. and Bernhard, R. 2019. How to use mixed-methods and triangulation designs: An introduction to history education research. History Education Research Journal, Vol. 16, No. 1, pp. 5-23. Accessed 31 May, 2020 at https://doi.org/10.18546/HERJ.16.1.02

Klein, H. and Myers, M. 1999. A set of principles for conducting and evaluating interpretive field studies, MIS Quarterly, Vol. 23, No. 1, pp. 67-93.

Krauss, S. 2005. "Research Paradigms and Meaning Making: A Primer", *The Qualitative Report*, Vol.10, No. 4, pp. 758-770, 2005.

Katzenbeisser, S. and Petitcolas, F. A. 2000. *Information Hiding: Techniques for Steganography and Digital Watermarking*, Artech House, Computer Security Series, ISBN: 1-58053-035-4.

Kuhn, T. 1977. *The Essential Tension: Selected Studies in Scientific Tradition and Change*, Chicago, IL, University of Chicago Press.

Kuhn, T. 1996. The structure of scientific revolution, university of Chicago Press, Chicago.

Kwak, Y. et al. 2012. "Understanding End-users' Acceptance of Enterprise Re- source Planning (ERP) System in Project-based Sectors", *IEEE Transactions on Engineering Management*, Vol. 59, No. 2. Accessed June 09, 2017 at www.library.ukzn.ac.za

Kwon, T. 2011. "Privacy Preservation with X.509 Standard Certificates", In- formation Sciences, Vol. 181. Accessed on 16 January, 2016 at www. library.ukzn.ac.za

Latour, B. 1991. Technology is society made durable, in A sociology of monsters: essays on power, technology and domination, J. Law (ed), Routledge, London, pp. 103-131.

Le Compte, M. and Schensul, J. 1999. "Analysing and Interpreting Ethno- graphic Data", in *Book*
Five of The Ethnographer's Toolkit, Schensul, J. J. & Le Compte (Eds.) Walnut Creek, CA, Altamira Press, Sage Publications.

Lee, A. 1991. Integrating positivist and interpretive approaches to organizational research. Organization science. Vol. 2, No. 4, pp. 342-365.

Lee, C. and Tsai, W. 2012. "A Secret-sharing-based Method for Authentication of Grayscale Document Images via the Use of the png Image with a Data Repair Capability", IEEE Transactions on Image Processing, Vol. 2, No. 1. Accessed January 16, 2016 at www.library.ukzn//ieeexplore.ieee.org

Leech, N.L., Dellinger, A.M., Brannagan, K.B., Tanaka, H., 2010. Evaluating mixed research studies: a mixed methods approach. Journal of Mixed Methods Research 4 (1), 17–31.

Leonard-Barton, D. 1988. “Implementation Characteristics of Organization Innovations, Limits and Opportunities for Managerial Strategies”, *Communications Research*, Vol. 15, No. 5, pp. 603-631.

Lescevica, M., Ginters, E. and Mazza, R. 2013. “Unified Theory of Acceptance and Use of Technology (UTAUT) for Market Analysis of FP7 CHOReOS Products”, *Procedia Computer Science*, Vol. 26. Accessed June 10, 2017 at www.library.ukzn.ac.za

Livari, J. 1983. Contributions to the theoretical foundations of systemeering research and the picoco model, Institute of data processing science, University of Oulu, Oulu, Finland.

Lukkarinen, H., 2005. Methodological triangulation showed the poorest quality of life in the youngest people following treatment of coronary artery disease: a longitudinal study. International Journal of Nursing Studies 42 (6), 619–627.

Makgoba, M. and Mubangizi, J. 2010. The creation of the University of KwaZulu-Natal: Reflections on a merger and transformation experience. Excel Books, New Delhi, India.

March, S. and Smith, G. 1995. Design and natural science research on information technology, decision support systems, Vol. 15, pp. 251-266.

Marshall, C. and Rossman, G. 1999. *Designing Qualitative Research*, Edition 3, Sage Publications, London.

Massey J. L. and Omura, J. K. 1986. *Method and Apparatus for Maintaining the Privacy of Digital Messages Conveyed by Public Transmission*, US Patent US4567600A. https://patents.google.com/patent/US4567600

Maxwell, J. 1992. “Understanding and Validity in Qualitative Research”, *Harvard Educational Review*, Vol. 62, No. 3, pp. 279-299.

McNabb, D. 2004. *Research Methods for Political Science: Quantitative and Qualitative Methods*, Armonk, M. E. Sharpe Inc., New York.

Mead, G. H. 1934. *Mind, Self and Society*, University of Chicago Press. Accessed January 16, 2016 at https://scholar.google.com

Menezes, A., Van Oorschot, P. and Vanstone, S. 1996. *Handbook of Applied Cryptography*, CRC Press, pp. 500-642, ISBN: 0-8493-8523-7.

Merriam, S. B. 1998. *Qualitative Research and Case Study Application in Education: Revised and Expanded from Case Study Research in Education*, Jossey- Bass, San Francisco. Mertens, D. 2005. *Research and Evaluation in Education and Psychology*, Edition 2, Sage, London.

Metcalfe, M. 2008. “Pragmatic Inquiry”, *Journal of the Operational Research Society*, Vol. 59, pp. 1091-1099. Accessed January 30, 2016 at www.library. ukzn.ac.za

Midtgaard, J., Rorth, M., Stelter, R., Adamsen, L., 2006. The group matters: an explorative study of group cohesion and quality of life in cancer patients participating in physical exercise intervention during treatment. European Journal of Cancer Care 15 (1), 25–33.

Miles, M. B. & Huberman, A. M. 1994. *Qualitative Data Analysis* Thousand Oaks, Sage, CA.

Miles, M. and Huberman, A. 1994. An expanded sourcebook qualitative data analysis, (2nd ed), Sage Publications, Thousand Oaks, CA.

Mingers, J. 2001. Combining IS Research Methods: towards a pluralist methodology, information systems research, Vol. 12, No. 3., pp. 240-259.

Mishler, E. 1986. *Research Interviewing: Context and Narrative*, Harvard University Press, Cambridge, MA.

Morgan, D. 1997. *Focus Groups as Qualitative Research*, Edition 2, Sage Publications.

Morgan, D.L., 2007. Paradigms lost and pragmatism regained: methodological implications of combining qualitative and quantitative methods. Journal of Mixed Methods Research 1 (1), 48–76.

Morgan, D. 2018. Commentary-After triangulation, what next?. Accessed May 31, 2020 at https://doi.org/10.1177/1558689818780596

Morrison, J. and George, J. 1995. Exploring the software engineering component in MIS research, communications of the ACM, Vol. 38, No. 7, pp. 80-91.

Morse, J. 1994. *Critical Issues in Qualitative Research Methods*, Thousand Oaks, Sage, CA.

Mukwevho, J. and Jacobs, L. 2012. "The Importance of the Quality of Electronic Records Management in Enhancing Accountability in the South African public Service: A Case Study of a National Department", *Unisa Press* Mousaion Vol. 30, No. 2), pp. 33-51. Accessed January 16, 2016 at: www.library.ukzn. ac.za

Myers, M. 1997. "Qualitative Research in Information Systems", *MIS Quarterly*, Vol. 21, No. 2, pp. 241-242.

Nasri, W. and Charfeddine, L. 2012. "An Exploration of Facebook.com Adoption in Tunisia using Technology Acceptance Model (TAM) and Theory of Reasoned Action (TRA)", *Interdisciplinary Journal of Contemporary Research in Business*, Vol. 4, No. 5. Accessed June 09, 2017 at www.library.ukzn. ac.za

Newman,W. 1999. Social Research Methods. 4th ed. Allyn and Bacon, Boston.

Ngwenyama, O. and Lee, A. 1997. Communication richness in electronic mail: critical social theory and the contextuality of meaning, MIS Quarterly, Vol. 21, No. 2, pp. 145-167.

Nkwanyana, K. 2014. *The Statement by the Minister of Higher Education and Training on*

Fraudulent Qualifications in South Africa, Pretoria: Ministry Higher Education and Training, Republic of South Africa. Retrieved January 17, 2016 from www.news24.com

Obeng-Odoom, F. 2013. "Africa's Failed Economic Development Trajectory: A Critique", *African Review of Economics and Finance*, Vol. 4, No. 2. Accessed 17, January 2016 at www.library.ukzn.ac.za

O'Cathain, A., 2009. Reporting mixed methods projects. In: Andrew, S., Halcomb, E.J. (Eds.), Mixed Methods Research for Nursing and the Health Sciences. Wiley-Blackwell, Chichester, pp.
135–158.

O'Cathain, A., Murphy, E., Nicholl, J., 2007. Why, and how, mixed methods research is undertaken in health services research in England: a mixed methods study. BMC Health Services Research 7, 85.

O'Cathain, A., Murphy, E., Nicholl, J., 2008. The quality of mixed methods studies in health services research. Journal of Health Services Research & Policy 13 (2), 92–98.

Olsen, M., Lodwick, D. and Dunlop, R. 1992. *Viewing the World Ecologically*, Westview Press Boulder, CO.

Onwuegbuzie, A., Teddlie, C., 2003. A framework for analyzing data in mixed methods research. In: Tashakkori, A., Teddlie, C. (Eds.), Handbook of Mixed Methods in social & Behavioural Research. Sage, Thousands Oak, pp. 351–383.

Onwuegbuzie, A.J., Leech, N.L., 2005. On becoming a pragmatic researcher: the importance of combining quantitative and qualitative methodologies. International Journal of Social Research Methodology 8 (5), 375–387.

Orlowski, W. and Robey, D. 1991. Information technology and the structuring of organizations, information systems research, Vol. 2, No. 2, pp. 143-169.

Parameswaran, S., Kishore, R., and Li, P. 2015. "Within-study Measurement In- variance of the UTAUT Instrument: An Assessment with User Technology Engagement Variables", *Information and management*, Vol. 52. Accessed June 10, 2017 at www.library.ukzn.ac.za

Patton, M. Q. 2002. *Qualitative Research and Evaluation Methods*, Edition 3 Thousand Oaks, CA, Sage Publications.

Pearson, K. 1900. Karl Pearson's early statistical papers Cambridge University Press, pp.339-357. Accessed June 20, 2020 at www.googlescholar.com

Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G. 1999. "Information Hiding: A Survey", *Proceedings of the IEEE (special issue)*, Vol. 87, No. 7, 1062-1078.

Rafat, K. and Sher, M. 2013. "Secure Digital Steganography for ASCII Text Documents", *Arab Journal of Science engineering*, International Islamic University, Islamabad, Parkistan. Accessed January 16, 2016 from www. library.ukzn.ac.za

Raggo, M. T. and Hosmer, C. 2012. "Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols", Syngress. ISBN-13: 9781597497435.

Ragin, C. 1992. "Casing and the Process of Social Inquiry", in Ragin C. C. & H. S. Becker (Eds.), *What is a Case? Exploring the Foundations of Social Inquiry*, pp. 217-226, Cambridge University Press, Cambridge, UK.

Redelinghuys, J. 2013. *Are there Different Degrees of CV Fraud?*. Accessed January 16, 2016, from: www.dailymaverick.co.za/opinionsta/2013-06-30-are-there-different-degrees-of-cv-fraud/#.VTUPMwzkYy4

Reeves, T. & Hedberg, J. 2003. *Interactive Learning Systems Evaluation*, Educational Technology Publications, Englewood Cliffs, NJ.

Robey, D. 1996. Research commentary: diversity in information system research: threat, promise, and responsibility, Information Systems Research, Vol. 7, No. 4, pp. 400-408.

Robson, C. 2002. *Real World Research*, Edition 2, Oxford, Chapman & Hall.

SA Government, *South Africa's National Research and Development Strategy*, 2002. Accessed January 16, 2016 from South Africa's National Research and Development Strategy http://www.info.gov.za/otherdocs/2002/rd_ strat.pdf

Sakurai, K. and Shizuya, H. 1998. "A Structural Comparison of the Computational Difficulty of Breaking Discrete Log Cryptosystems", *Journal of Cryptology*, vol. 11, pp. 29-43.

Sale, J.E.M.,Lohfeld, L.H., Brazil, K., 2002. Revisiting the quantitative- qualitative debate: implications for mixed methods research. Quality and Quantity 36, 43–53.

Satir, E. and Isik, H. 2012. *A Huffman Compression Based Text Steganography Method*, Multimed Tools Application, LLC: Science plus Business Media. Accessed on 01, March 2015 at http://www.ukzn.ac.za

Saunders, M. Lewis, P. and Thornhill A. 2007. *Research Methods for Business Students* Prentice Hall.

Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance, 2011. Accessed on 16 January, 2016 at www.library. ukzn.ac.za

Shad, A. 2011. *Applications of Steganography*, MSc Thesis, A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in software engineering. California State University, Northridge.

Shannon, C. 1949. *Communication Theory of Secrecy Systems*, emphBell System Technical Journal, Vol. 28.

Shipman, C., Burt, J., Ream, E., Beynon, T., Richardson, A., Addington-Hall, J., 2008. Improving district nurses' confidence and knowledge in the principles and practice of palliative care. Journal of Advanced Nursing 63 (5), 494–505.

Shneiderman, B. and Plaisant, C. 2005. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*, Edition 4, Addison-Wesley, New York.

Simon, H.A., *The Sciences of the Artificial*, Edition 3, MIT Press, Cam- bridge, MA, 1988.

Siponen, M. and Baskerville, R. 2018. Intervention effect rates as a path to research relevance: information systems security example, "Journal of the Association for Information Systems: 19 (4). Accessed on 10, June 2020 at https:aisle.aisnet.org/jais/vol19/iss4/4?

Skilbeck, J.K., Payne, S.A. 2005. Ingleton, M.C., Nolan, M., Carey, I., Hanson, A.. An exploration of family carers' experience of respite services in one specialist palliative care unit. Palliative Medicine 19 (8), 610–618.

Steckler, A., McLeroy, K.R. 1992. Goodman, R.M., Bird, S.T., McCormick, L. Toward integrating qualitative and quantitative methods: an introduction. Health Education Quarterly 19 (1), 1–8.

Smith, A. 1999. *Why digitize?*, Council on Library and Information Resources. Washington, DC. Accessed on 02, June 2016 at www.google.scholar. com

South African Government Information, *Strategic Plan 2011 - 2014*, Department of Communications, 2011. Accessed January 16, 2016 from South African Government Information http://www.info.gov.za/view/ DownloadFileAction?id=144159

Stake, R. E. 1995. *The Art of Case Study Research*, Sage Publications, Thousands Oak, CA. Strauss, A. and Corbin, J. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, Sage Publications, Newbury Park, CA, 1990.

Su, P. 2003. Information Hiding in Digital Images: Watermarking and Steganography, PhD Thesis, University of Southern California.

Sumak, B., Hericko, M, Pusnik, M. and Polancic, G. 2011. "Factors Affecting Acceptance and Use of Moodle: An Empirical Study Based on TAM", *Slovenian Society Informatika*, Vol. 35, No. 1, 2011, in Wong, K. et.al. 2013. Understanding Student Teachers' Behavioural Intention

to use Technology: Technology Acceptance Model (TAM) Validation and Testing, *International Journal of Instruction*, Vol. 6, No. 1. Accessed January 17, 2016 at www.library.ukzn.ac.za

Tashakkori, A., Creswell, J.W. 2007. Editorial: the new era of mixed methods. Journal of Mixed Methods Research 1 (1), 3–7.

Tashakkori, A., Teddlie, C., 2003. Handbook of Mixed Methods in Social & Behavioural Research. Sage, Thousands Oak.

Tellis, W. 1997. "Introduction to Case Study: The Qualitative Report", Vol. 3, No. 2. Accessed June 29, 2016, from: http://www.nova.edu/ssss/QR/ QR3-2/tellis1.html

Teo, T. 2011. "Factors Influencing Teachers' Intention to Use Technology: Model Development and Test", Computers & Education, in Wong, K. et.al. 2013. Understanding Student Teachers' Behavioural Intention to Use Technology: Technology Acceptance Model (TAM) Validation and Testing, *Inter- national Journal of Instruction*, Vol. 6, No. 1, Accessed January 17, 2016 at www.library.ukzn.ac.za

Teo, T., 2010. "Efficiency of the Technology Acceptance Model to Explain Pre- service Teachers' Intention to Use Technology: A Turkish Study", *Campus Wide Information System*, Vol. 28, No. 2, in Wong, K. et.al. 2013. Understanding Student Teachers' Behavioural Intention to Use Technology: Technology Acceptance Model (TAM) Validation and Testing, *International Journal of Instruction* Vol. 6, No. 1. Accessed January 17, 2016 at www. library.ukzn.ac.za

Teo, T. and Noyes, J. 2011. "An Assessment of the Influence of Perceived Enjoyment and Attitude on the Intention to Use Technology Among Pre-service Teachers: A Structural Equation Modelling Approach", *Computer and Technology*, Vol. 57, No. 2, in Wong, K. et.al. 2013. Understanding Student Teachers' Behavioural Intention to Use Technology: Technology Acceptance Model (TAM) Validation and Testing, *International Journal of Instruction*, Vol. 6, No. 1. Accessed January 17, 2016 at www.library.ukzn.ac.za

Teo, T., Wong, S., and Chai, C. 2008. "A Cross-cultural Examination of the Intention to use Technology Between Singaporean and Malaysia Pre-service Teachers: An Application of the TAM. Educational and Society", Vol. 11, No. 4, in Wong, K. et.al. 2013. Understanding Student Teachers' Behavioural Intention to Use Technology: Technology Acceptance Model (TAM) Validation and Testing, *International Journal of Instruction*, Vol. 6, No. 1. 2008. Acccessed
January 17, 2016 at www.library.ukzn.ac.za

TerreBlanche, M. & Durrheim, K., *Research in Practice*, UCT Press, Cape Town, 1999.

The (UK) National Archives, *Regulation of Investigatory Powers Act 2000*, 2000. https://www.legislation.gov.uk/ukpga/2000/23/contents

UNESCO,*Science Policy and Capacity Building*, 2012. Accessed January 16, 2016, at:UNESCO:http://www.unesco.org/new/en/natural-sciences/science-technology/universityindustry-partnerships/science-parks-around-the-world/science-parks-in-africa

United Nations, *Statistical Annex*, 2013. Accessed January 16, 2016 at https://scholar.google.co.za

University of KwaZulu-Natal Website, 2016. Accessed January 12, 2016 at www.ukzn.ac.za

University of Toronto, BRICS Information Centre, 2012. Accessed January 16, 2016 from: University of Toronto: http://www.brics.utoronto.ca

Venkatesh, V. 2000. "Determinants of Perceived Ease of Use Integrating Control, Intrinsic Motivation and Emotion into the Technology Acceptance Model", *Information Systems Research*, Vol. 11, No. 4, in Wong, K. et.al. 2013 Understanding Student Teachers' Behavioural Intention to use Technology: Technology Acceptance Model (TAM) Validation and Testing, *International*

Journal of Instruction, Vol. 6, No.1. Accessed January 17, 2016 at www. library.ukzn.ac.za

Venkatesh, V. and Davis, F. 2000. "A Theoretical Extension of Technology Acceptance Model: Four Longitudinal Field Studies", *Management Science*, Vol. 46. Accessed January 17, 2016 at www.library.ukzn.ac.za

Venkatesh, V. Morris, M. Davis, G. and Davis, F. 2003. "User Acceptance of Information Technology: Toward a Unified View", *MIS Quaterly*, Vol. 27, No. 3. Accessed January 17, 2016 at www.library.ukzn.ac.za

Venkatesh, V., Brown, S., and Bala, H. 2013. "Bridging the Qualitative- quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems", *MIS Quarterly*, Vol. 37, No. 1. Accessed June 09, 2017 at www.library.ukzn.ac.za

Vorster, A. 2014. *Safeguarding the Integrity of Secure Documents*, Graphix, May/June 2014. Accessed November 12, 2016 from www.sappi.securitypapers.com

Walsham, G. 1993. *Interpreting Information Systems in Organizations*, John Wiley, Chichester. Accessed January 29, 2017, from www.library.ukzn. ac.za

Wolcott, H. F. 1990. *Writing up Qualitative Research*, Sage Publications, Newbury Park, CA.

Wong, S. and Teo, T. 2009. “Investigating the Technology Acceptance Among Student Teachers in Malaysia: An Application of the Technology Acceptance Model (TAM)”, *The Asia-Pacific*
Education Researcher, Vol. 18, No. 2. Accessed January 17, 2016 at www.library.ukzn.ac.za

Wong, K., Teo, T. and Russo, S. 2012. “Influence of Gender and Computer Teaching Efficacy on Computer Acceptance Among Malaysian Student Teach- ers: An Extended Technology Acceptance Model”, *Australasian Journal of Educational Technology*, Vol. 28, No. 7. Accessed June 10, 2017 at www.library.ukzn.ac.za

Wong, K. et al. 2013. “Understanding Student Teachers’ Behavioural Intention to Use Technology: Technology Acceptance Model (TAM) Validation and Testing”, International Journal of Instruction. Vol. 6, No. 1. Accessed June 10, 2017 at www.library.ukzn.ac.za

Wu, H., and Volker, D. 2009. The use of theory in qualitative approaches to research: application in end-of-life studies. Journal of Advanced Nursing 65 (12), 2719–2732.

Wu, H., and Volker, D. 2009. The use of theory in qualitative approaches to research: application in end-of-life studies. Journal of Advanced Nursing 65 (12), 2719–2732.

Xie, H. 2008. “Users’ Evaluation of Digital Libraries (DLs): Their Uses, Their Criteria and Their Assessment”, *Information Processing and Management*, Vol. 44, pp. 1346-1373.
Accessed on June 02, 2016 at www.google. scholar.com

Xiaoying, F. and Behar-Horenstein, L. 2019. Maximizing Nvivo utilities to analyse open-ended responses. Accessed June 10, 2020 at https://nsuworks.nova.edu/tqr/vol24/iss3/11/

Yin, R. 2008. *Case Study Research*, Saga Publications, Thousand Oaks, CA.

Yin, R. K. 2003. *Case Study Research: Design and Methods*, Edition 3, Sage Publications, Thousand Oaks. Accessed January 29, 2017 from www. library.ukzn.ac.za

Yin, R. 1994. *Case Study Research: Design and Methods*, Thousand Oaks, CA, Sage Publications.

Zawilska, A., 2012. *Qualifying Steganographic Embedding Capacity in DCI-based Embedding Schemes*, University of KwaZulu-Natal, School of Electrical, Elec- tronic and Computer Engineering. Accessed January 29, 2017, from: www.researchspace.ukzn.ac.za

Zepke, N. and Leach, L. 2011. “Engaging Students in Learning: A Review of a Conceptual Organizer”, *Higher Education Research and Development*, Vol. 30, No. 2. Accessed on 20 June, 2017 at www.library.ukzn.ac.za

Appendix A

SURVEY OPINION OF INNERWEB

Survey opinion of

I, Philisiwe Joyce Myeza am a Phd student in the School of Information systems, at the University of

KwaZulu-Natal. This questionnaire aims to collect participants' opinion of using innerweb. Innerweb is a portal that provides staff of UKZN with access to information and resources. This study serves as a means to measure the determinants in the usage of innerweb and serves as a basis to provide recommendations for continuous improvement to innerweb implementation and development. All data collected will be used for statistical and research purposes only and will be kept strictly confidential. Your participation in this survey is purely

Demographic data
Please select the choice answer that best defines your situation.

Do you think archiving and securing information is part of your job?

- Yes
- No

How would you rate your computer knowledge?

- Very Little
- Fair
- Good
- Expert

Are you familiar with Innerweb?

- Yes
- No
- Not sure

What task do you perform on Innerweb?

- Uploader of information
- End User of the System
- Both of the above

How often do you use Innerweb?

- Everyday
- Once in a while
- Seldom
- Not sure

On average, for the past six months how long would you be logged onto Innerweb?

- Less than an hour
- More than an hour
- None

On average, how long do you spend logged onto the innerweb every time you log in?

- Less than an hour
- More than an hour
- Not sure

How long have you worked at the University of KwaZulu-Natal?

- Less than a year
- Between one and five years
- More than five years

Your Gender
Choose one of the following answers

- Female
- Male

Your Age

- 21 years and below
- Between 22 to 40 years
- 41 years and above

If I use the Innerweb I will increase my chances of achieving better performance in my operations

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

Using the Innerweb system increases my productivity.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

I find the Innerweb system useful

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

Using the Innerweb system enables me to accomplish tasks more quickly.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

My interaction with the Innerweb system would be clear and understandable.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

Learning to operate the Innerweb system is easy for me.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

People who are important to me think i should use the Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

People who are important to me have been helpful ion the use of Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

In general, my organization has supported the use of Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

The Innerweb system is compatible with other systems I use.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

I have the knowledge necessary to use the Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

- I have the resources necessary to use the Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

A specific person or group is available for assistance with Innerweb system difficulties.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

It will be easier for me to become skillful at using the Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

I would find the Innerweb system easy to use.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

It will be easier for me to become skillful at using the Innerweb system.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

I would find the Innerweb system easy to use.

- Strongly disagree
- Disagree
- Agree
- Strongly agree
- N/A

Appendix B

Proposed Method for Securing and Archiving

B.1 Introduction:

In this chapter, the basic method used for the security of e-certificates and other e-documents through encryption and hiding (in other image files) is discussed, and example results of the potential use in UKZN, presented. The material is based on the works of Blackledge et al. [Bla17], [Bla19]. As a researcher, I acknowledge at this point that my expertise does not extend to algorithms, which form a central part of this chapter. Similarly, of necessity, there is a fair input from Mathematics required here. My expertise is in some programming languages like css and html. While this is of some assistance in this research, I relied on MATLAB for this analysis, and what I include is generated from MATLAB which is a computer programming language. MATLAB has been used to generate the codes which are found on the appendix of this thesis. The following programmers were responsible for generating these MATLAB codes and I would like to acknowledge their contribution: (Professor Jonathan Blackledge, Honorary Professor, Dublin Institute of Technology, Ireland. Distinguished Professor Warsaw University of Technology, Poland. Professor Extraordinaire, University of Western Cape, South Africa. Professor Cid Mathew Adolfo, Department of Systems Engineering, Military Technological College, Ministry of Defence, Oman. Professor Paul Tobin, School of Electrical and Electronic Engineering, Dublin Institute of Technology, Ireland).

The discussion in this chapter is a collaborated contribution of Professor Jonathan Blackledge, Honorary Professor, Dublin Institute of Technology, Ireland. Distinguished Professor Warsaw University of Technology, Poland. Professor Extraordinaire, University of Western Cape, South Africa. Professor Cid Mathew Adolfo, Department of Systems Engineering, Military Technological College, Ministry of Defence, Oman. Professor Paul Tobin, School of Electrical and Electronic Engineering, Dublin Institute of Technology, Ireland and Philisiwe Joyce Myeza, Director of Libraries at UKZN. This discussion is found in a published paper “Information hiding with data diffusion using convolutional encoding for super-encryption for publication in 2018.

The unification of data encryption with information hiding methods continues to receive significant attention because of the importance of protecting encrypted information by making it covert. This is because one of the principal limitations in any cryptographic system is that encrypted data flags the potential importance of the data (i.e. the plaintext information that has

been encrypted), possibly leading to the launch of an attack which may or may not be successful. Information hiding overcomes this limitation by making the data (which may be the plaintext or the encrypted plaintext) imperceptible, the security of the hidden information being compromised if and only if, its existence is detected.

Information or data hiding is the process of embedding and usually concealing data in similar or different forms of other data so that the hidden information is protected from unauthorized access [Pet99], and embraces the principles associated with Watermarking and Stenography [Cox07]. The term 'Information Hiding' can refer to either making the information imperceptible or keeping the existence of the information secret. In computer science, it refers to the 'ability to prevent certain aspects of a software component from being accessible to its clients, using either programming language features (like private variables) or an explicit exporting policy', [Wik18], [Rag12].

The development of techniques for hiding information is important in situations when the use of data encryption is not feasible or when encryption cannot assure data security due to the encrypted information arousing suspicion or when the transmission of encrypted information is incriminating (e.g. in situations when the transmission of encrypted information is banned, is illegal or subject to investigatory powers [RIP00]). Information hiding techniques embed plaintext data into covertext data that one wishes to send secretly via an innocuous 'message' based on the transmission of so-called stegotext data, which should be in a form that restricts detection or recovery of the hidden data. There are two principal data hiding categories, namely, Watermarking and Steganography [79].

Watermarking is the process of embedding information into another medium in a way that is difficult to remove, which is useful to protect the source of the information and avoid copyright violation, amongst other things. An example of this concept is visible watermarking where the watermark is visible in the media used, such as a text or logo which identifies the owner of the media. Other classes of watermarking include invisible watermarking, in which the information is added to the media in such a way that it cannot be recognized. Digital watermarking systems can be further categorized according to the robustness of an attack into fragile, semi-fragile and robust, and can be used for copyright protection, source tracking or covert communications.

Stenography is the 'art' of embedding secret data into other data in such a way that no one, apart from the sender and intended recipient, suspects the existence of the secret data. The more recent use of this concept has emerged with the rapid development and communication of digital images, videos, and audio files which can be used as a medium for embedding important data. In other words, we currently live in a 'covertext rich environment' which is one of the principal reasons for the interest in, and, the development of, new steganographic techniques.

The main advantage of Steganography is that messages do not attract attention to themselves and an examination of the data does not immediately reveal the existence of hidden information. Thus, with regard to a one-to-one communication protocol, the user sending the hidden data and the recipient of the data are the only 'users' who know about the existence of the hidden data. Many steganographic techniques have been proposed, but steganography can be categorized into three basic types: (i) pure steganography, in which the sender embeds the secret data directly, and the receiver extracts it likewise; (ii) private-key steganography, where the sender uses a private key to embed the secret information in a way that is similar to private-key encryption and (iii) public-key steganography, in which the sender embeds the secret data using a private-key and the receiver extracts it using a public-key, a process that is similar to the public-key encryption.

Steganocryptography is a combined form of cryptography and steganography in which the data to be hidden is first encrypted before it is hidden in the covertext. This can pose certain restrictions on the way in which the encrypted data is hidden and requires that the extraction of the hidden cipher is achieved with minimal error so that an accurate decrypt can be obtained. This condition usually limits the robustness of the stegotext to transmission noise and other forms of distortion, i.e. the hidden encrypted data becomes fragile. On the other hand, it makes the stegotext tamperproof, thereby giving the receiver evidence of an intercept and negating the potential for a decrypt to include disinformation that is taken by a recipient to be genuine. Most methods are divided into two categories: the first category focuses on embedding encrypted data in the spatial domain, whereas the second category is based on the use of a transform domain to hide encrypted information. The latter approach is taken, the method developed being exclusively based on an application of the Fourier transform.

The approach reported in this thesis considers a variation on the theme of convolutional encoding which involves two principal processes, namely, 'Data Diffusion' and 'Stochastic Diffusion', the latter method having been researched and implemented in a number of previous publications, e.g. [Bla09], [Bla10], [Bla11], [Bla13] and [Raw14]. These processes are used to develop a highly fragile and thereby tamper-proof method of hiding encrypted data in host data fields. The approach considered, which utilizes the properties and characteristics of the Fourier transformation and the convolution and correlation integrals, is developed for arbitrary dimensions so that applications of the method can be used for encrypting and hiding information in digital signals, digital images and for three- and four-dimensional (i.e. three-dimensions + time) signal processing applications. An example is presented in a case study that focuses on encrypted full-colour image information hiding with applications that can include image and edocument authentication, copyright protection and covert encryption for which prototype software is provided in Appendix B using m-code.

B.2 Basic Approach

The initial process of encryption and decryption requires two digital images I_1 (the plaintext) and I_2 (the covertext) of type real, each of which are regular matrices of size N×M whose elements are composed of floating point values between 0 and 1 inclusively (typically obtained by conversion to normalised floating point form from a *k*-bit image). The detailed analysis of how the encryption and decryption happens is provided in Appendix B which consist of Section B1 for Encryption and Section B2 for Decryption. And the function which is for the execution of both encryption and decryption is found on Section B3.

A plaintext image I_1 is encrypted using both data and stochastic diffusion and the output hidden in covertext image I_2 generating a stegotext image I_3,

There are mathematical equations for these models copied as they are from the experts. (See the detailed processes in Appendix B).

All processes are applied separately to each of the RGB components of the colour input images and the keys for encrypting I_1 are derived from the covertext image I_2. Both images are processed as images of the same size. However, upon input, the images can be of a different exact size, although it is assumed that they are of the same order of magnitude in size (and therefore resolution) and have a similar perspective, the format of the input images being of any type part and typically assumed to be JPEG images.

The method assumes the use of floating point arithmetic throughout including writing the stegotext image to file. For this reason, a Tagged Image File Format is considered in which the floating point data is retained. This is a fundamental requirement in order to recover the data prior to application of the inverse processes required to output a decrypt which is highly sensitive to (floating point) errors introduced into the stegotext, thereby making the approach tamper-proof, i.e. floating point errors (subject to the floating point accuracy of the computations) introduced into the stegotext image through transmission noise or inspection by an attacker, including quantization of the image, for example, leads to an erroneous decrypt.

B.3 Encrypted Certificate Hidden in Holders Portrait

Figure 6.1 shows an example of the application of the m-code given in Appendix B, in particular the I/O associated with function **Encrypt**.

Similarly, Figure 6.2 shows the I/O associated with the operation of function **Decrypt**. Comparing the results, it is clear that the visual differences between I_2 and I_3 in Figure 6.1 are insignificant for the optimized value of the IEC used. Further, the visual differences between I_1 and I4 (comparing the plaintext in Figure 6.1 and the decrypt in Figure 6.2) is also insignificant, and can be used to validate (or otherwise) the details given in the certificate. Diffusion of the images I1 and I2 is undertaken by function Image Diffusion (as given in Appendix B: Section B3) using the MATLAB Fast Fourier Transform algorithm fft2, the inverse process being accomplished using function Inverse Image Diffusion (see Appendix B: Section B3).

Figure 9. 2: Example of the application of function Encrypt: Plaintext image (left) I_1, Covertext image (middle) I_2, Stegotext .tiff image (right) I_3.

Figure 9. 3: Example of the application of function Decrypt: Stegotext image (left) I_3, Covertext image (middle) I_2 and decrypt (right) I_4.

B.4 Encrypted Certificate Hidden in the Same Certificate

Another example is given in Figures 6.3 and 6.4, which show an example of the selfauthentication of an academic certificate.

Figure 9. 4: Example of the application of function Encrypt for self-authentication of a certificate: Plaintext image (left) I_1, Covertext image (middle) I_2, Stegotext.tiff image (right) I_3.

Figure 9. 5: Example of the application of function Decrypt for the self- authentication of a certificate: Stegotext image (left) I_3, Covertext image (middle) I2and Decrypt image (right) I_4.

The stochastic function S given in Equation (6.1) used to encrypt the plaintext is computed using the MATLAB function rand, which returns a uniformly distributed matrix of pseudo-random floating point numbers, with floating point values between 0 and 1 inclusively. However, it is well known that functions such as MATLAB rand, which is based on 'Mersenne Twister', and conventional linear congruential methods of pseudo-random number generation, are cryptographically weak. Thus, in 'field operations' of the method discussed, the rand function should be based on pseudo- random number generators that are known to be cryptographically strong, and, ideally, personalized algorithms using new classes of chaos-based algorithms obtained through the application of Evolutionary Computing and/or Artificial Intelligence, for example [Tob13] and [Tib15].

The rand function is used in functions Stochastic Diffusion which implements the convolution encoding process using Equation (6.1) and Inverse Stochastic Diffusion which recovers the data via application of Equation (6.2) using the same key(s) to set the 'state' (the initial condition) of the pseudo-random number generator. While these keys can be generated independently by the user, because the covertext image is critical to computing the decrypt, the covertext is used to generate the keys directly.

It is envisaged that in the routine application of this algorithm, and given that the keys used for stochastic diffusion are derived from the covertext, the sender and receiver of the stegotext would agree a priori upon a database of covertext images. Since the visual difference between the stegotext and covertext is insignificant, a visual inspection of the database using Thumbnails ensues. Thumbnails are reduced-size versions of the images contained in a database which serves the same role for images as a normal text index does for words as used by most modern operating systems or desktop and mobile environments. They would be used to decrypt the encrypted image contained in the stegotext by the user choosing the image in the database that matches the received covertext. For large image databases, visual search engines could be used to produce a 'stegotextcovertext match'.

B.5 Covertext Exchange

The application of function Encrypt and Decrypt is clearly dependent on both users of these function having access to the same covertext. In order to achieve this, algorithms have been designed to encrypt/decrypt images, using a phase-only encryption method based on the work of Blackledge et al. [Bla19], up where I1 is the plaintext, I2 is the encrypted image and S is a ciphertext characterized by a phase-only spectrum. The result that is independent of the value of c which allows the plaintext to be fully embedded in the cipher thereby eliminating the statistical signature of the plaintext.

An example of the application of this approach is given in Figure 6.5 for the exchange of the covertext used in Figure 5.1, using the function **POE** and **POD** given in Appendix C.

In order to use these functions, it is required that both users have knowledge of the keys used to encrypt the RGB components of the plaintext image. Thus, the final component of the system considered is based on using phase-only encryption to exchange the keys via implementation of a three-pass protocol as discussed in the following section

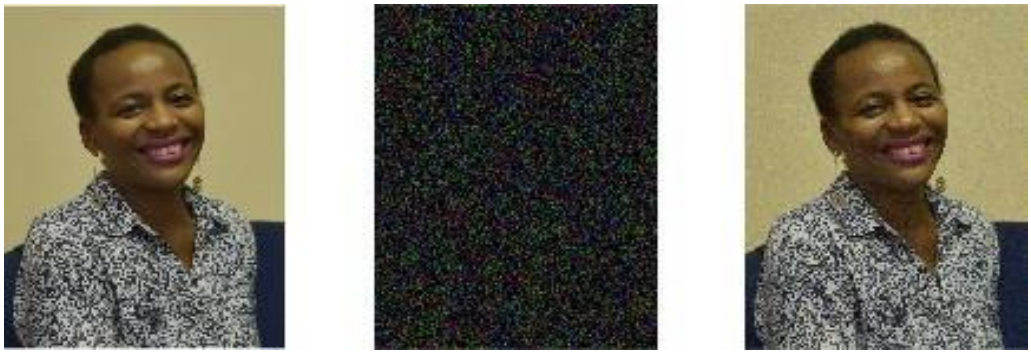


Figure 8. 6: Example of the application of function POE and POD: Plaintext image (left) I1, Ciphertext image I2 (middle) - Equation (6.3), Decrypted image I1 (right) - Equation (6.4). check

B.6 Key-exchange using a Three-pass Protocol

The Three-pass Protocol is well known and a range of algorithms have been developed for its implementation. These include the Shamir three-pass protocol [Men96] and the Massey-Omura method [Mas86]. The principle associated with the protocol is as follows: Alice encrypts her plaintext with a known algorithm and private key K_A, say, and sends the ciphertext to Bob. Upon receipt of the ciphertext, Bob cannot decrypt the cipherext because he does not know K_A. Instead Bob encrypts the cipherext using the same algorithm and a new private key K_B and sends the now double-encrypted plaintext back to Alice. Upon receipt, and critically, assuming the encryption algorithm is commutative, Alice can decrypt the double encrypted ciphertext with K_A and send the result (a single encrypted ciphertext) back to Bob, who is then able to decrypt the result using K_B. By using this protocol, Alice and Bob do not need to agree upon a K_A and K_B a priori and thus, no separate key exchange method is required.

Three principal conditions for the application of this protocol are required:

- Irrespective of the number of encryptions that take place, the encryption algorithm used must be both commutative and strong enough so that it cannot be broken using a known algorithm attack;
- the keys used must be of a sufficient length to make an exhaustive attack impracticable on any pass;
- if the encrypted information is intercepted for each of the three passes, it is not possible to determine the plaintext from the three intercepts (assumed to be complete in each case).

In practice, it is the third of the conditions that yields the greatest vulnerability, and any encryption system that exploits this protocol must be based on algorithms that exhibit a 'computational difficulty'. For example, in the case of the Shamir and Massey-Omura

algorithms, the security relies on the difficulty of computing discrete logarithms in a finite field, [Sak98].

Appendix D provides prototype software using MATLAB to implement the algorithm based on Equation (6.3) and Equation (6.4) for one-dimensional array processing using function **TPP**, an acronym for Three-pass Protocol which has been designed to transfer an array of integers between two users (Alice and Bob) in the form of an ASCII delimited file, which represents the initial plaintext - Plaintext.txt. The plaintext is typically a key which may be a concatenation of the keys used to execute the functions POE and POD given in Appendix C, for example. The function has three inputs:

- the *key* - a string of numbers between 0 and 9 - used by Alice for the first and third passes and a different key used by Bob for the second pass and the final decrypt;
- the step which is has input values 1 (first pass), 2 (second pass), 3 (third pass)
- and 4 (for the final decrypt);
- the Spectral Embedding Constant c which is required for the first pass (for step=1) only, i.e. $c >> 1$ is required to be set by Alice to produce the first ciphertext; the value of this constant is not required to be known by Bob and is not used for any other step other than step 1.

In each of the steps 1-3, the ciphertext is written to a file - 'Ciphertext.txt' - which is assumed to be sent (by email, for example) from Alice to Bob (step=1), from Bob back to Alice (step=2) and from Alice back to Bob (step=3). After step=3, Bob decrypts the ciphertext to recover the plaintext file which is output to the file 'Plaintext.txt'. In all cases, the MATLAB functions *'dmlread'* and *'dmlwrite'* are used for reading and writing the data to file, respectively.

By way of example, consider the exchange of a key given by the array 80 97 115 115 119 111 114 100, which is the ASCII decimal integer representation for the character string Password.

It is assumed that Alice creates a file called 'Plaintext.txt' containing the array of integer given. Alice runs the function (for *opt* = 1) **TPP(1234,1,123456789)**, where 1234 is Alice's key (known only to her) Alice then sets the value of c to 123456789 (also known only to Alice), for example (any value of c is valid up to the threshold associated with the precision used which is ideally required to be as quantified such as in Figure 3). After receipt of the file 'Ciphertext.txt' from Alice, Bob runs the function (for *opt* = 2) TPP(4321,2), where 4321 is Bob's key (known only to him) and sends the result - 'Ciphertext.txt' - back to Alice. After receipt of Bob's cipher, Alice runs the function **TPP(1234,3)** and sends the new ciphertext file - 'Ciphertext.txt' - back to Bob. Upon receipt of this file, Bob runs **TPP(4321,4)** to recover the key which is written in the output file 'Plaintext.txt'. Providing identical private keys are used by Alice and

Bob for steps 1 and 3 and steps 2 and 4, respectively, the output file will contain the integer array 80 97 115 115 119 111 114 100. Thus, Alice's key is passed to Bob using the Three-pass Protocol.

Given that the algorithms presented in Appendix C require three keys (for the Red, Green and Blue components), function **TPP** can be used to exchange these keys using a concatenated key: *key R 1 key G 1 key B*, where | denotes the concatenation of the arrays key R, key G and key B.

The components of the array associated with each key are then concatenated into a string for application in functions **POE** and **POD**, the length of the integer strings representing each component key being limited to 10 digits.

B.7 Discussion

With regard to the algorithms discussed in this chapter and presented in Appendix B, the attacker is first required to detect the existence of the encrypted information before an attempt can be made to decrypt it, the use of steganographic algorithms allowing for the existence of a ciphertext to be unknown. To recover the information, the attacker needs to first find a way of extracting the hidden encrypted information from the covertext and then decrypting it using the appropriate algorithm(s)/key(s). The exposure of the encryption key(s), the encryption algorithm(s) and the embedding technique to those other than the intended receiver, is practically impossible provided, given the design of the key generating algorithm used, the covertext is not compromised. In this context, greater security would be provided if the key(s), and, ideally the pseudo-random number generating algorithm used for stochastic diffusion, were generated independently from the covertext. This is, of course, at the cost of having to implement a separate key/algorithmexchange protocol, but under the fundamental cryptographic principle: *One message, one key, one cipher,* and/or, in regard to the work reported here, *one covertext.*

The applications of the approach considered are numerous. Coupled with appropriate keyexchange protocols to initiate the use of cryptographically strong ciphers, the approach provides a generic method of encrypting and hiding high fidelity digital information. The encrypted data is highly sensitive to transmission error and intolerant to distortion. The hidden data is therefore very fragile and hence, tamper-proof. This is due primarily to the method of information hiding, which relies on floating point addition so that truncation of the stegotext due to quantization involving transformation from floating point to integer form is not possible as is lossy compression. However, digital images commonly rely on 'depth-quantization' so that they can be displayed and retained as arrays composed of integers. This is why Least Significant Bit

methods are so popular in image- based steganography, a method which has not been applied in this case. Thus, a further investigation that would be of value is to consider different data embedding techniques other than the floating point additive approach considered here, which necessitates the output image file having to be written in floating point form (i.e. as in function Write **TIFF Image** given in Appendix B - Section B3).

Appendix C

PROTOTYPE MATLAB CODE FOR IMAGE STEGANOCRYPTOGRAPHY

This Appendix reports on the principal software developed for the evaluation of information hiding used in regard to the research undertaken in this thesis. Details of the approach taken is given in the publication information Hiding with Data Diffusion using Convolutional Encoding for Super-encryption available from http:

//www.e-hilaris.com/MA/2017/MA7_4_2.pdf

The software was developed and implemented using (64-bit) MATLAB R2017b with double precision floating point arithmetic. The functions provided have not been exhaustively tested.

C.1 Function to Encrypt Data

function Encrypt

```
%Read the colour images into arrays I1_C and I2_C, respectively
%noting that the mages are assumed to be of the same size.
I1_C=imread('Plaintext','bmp');
I2_C=imread('Covertext','bmp');
A=I1_C; B=I2_C;%Assign inputs to arrays A and B %Get
size of Covertext image A.
[rowsA colsA numberOfColorChannelsA]=size(A); %Get
size of Stegotext image B.
[rowsB colsB numberOfColorChannelsB]=size(B); %See
if lateral sizes match.
if rowsB ~= rowsA || colsA ~= colsB
%If size of A does not match B, resize A to match size of image
%B noting that image B - the Stegotext - must not be changed. A
= imresize(A, [rowsB colsB]); end
I1_C=A; I2_C=B;%Re-assign arrays to original variables
```

```
%Display plaintext and povertext images (as required).
figure(1), imshow(I1_C); figure(2), imshow(I2_C); %Extract the
RGB colour channels of both images.
I1_R =I1_C(:, :, 1); I1_G =I1_C(:, :, 2); I1_B =I1_C(:, :, 3);
I2_R =I2_C(:, :, 1); I2_G =I2_C(:, :, 2); I2_B =I2_C(:, :,
3);
[N,M]=size(I1_R);%Compute size of image arrays.
%Convert to normalised floating point form.
I1_R=im2double(I1_R); I1_G=im2double(I1_G);
I1_B=im2double(I1_B); I2_R=im2double(I2_R);
I2_G=im2double(I2_G); I2_B=im2double(I2_B);
%Diffuse RGB components of the plaintext and covertext images,
ID_R=Image_Diffusion(I1_R,I2_R,N,M);
ID_G=Image_Diffusion(I1_G,I2_G,N,M);
ID_B=Image_Diffusion(I1_B,I2_B,N,M); %and generate RGB keys.
[Key_R,Key_G,Key_B]=Key_Generation(I2_R,I2_G,I2_B); %Apply
Stochastic Diffusion (modified convolution coding).
SD_R=Stochastic_Diffusion(ID_R,N,M,Key_R);
SD_G=Stochastic_Diffusion(ID_G,N,M,Key_G);
SD_B=Stochastic_Diffusion(ID_B,N,M,Key_B);
%Hide RGB components of data into RGB components of covertext
%using optimised value of information embedding coefficient
c. c=0.0001; I3_R=Hide_Data(I2_R,SD_R,c);
I3_G=Hide_Data(I2_G,SD_G,c); I3_B=Hide_Data(I2_B,SD_B,c);
%Reconstruct colour stegotext image and display (as required). I
= cat(3,I3_R,I3_G,I3_B); figure(3), imshow(I); %Write stegotext
image to file as Tagged Image File Format noting
%that it is critical the data be retained in floating point
form. Write_TIFF_Image(I);
```

C.2 Function to Decrypt Data

function Decrypt

```
%Read covertext and stegotext images to arrays I2_C and I3_C
I2_C=imread('Covertext','bmp');
I3_C=imread('Stegotext.tif','tif'); A=I2_C; B=I3_C;%Assign
inputs to arrays A and B %Get size of Covertext image A.
```

```
[rowsA colsA numberOfColorChannelsA]=size(A); %Get
size of Stegotext image B.
[rowsB colsB numberOfColorChannelsB]=size(B); %See
if lateral sizes match.
if rowsB ~= rowsA || colsA ~= colsB
%If size of A does not match B, resize A to match size of image
%B noting that image B - the Stegotext - must not be changed.
A = imresize(A, [rowsB colsB]); end
I2_C=A; I3_C=B;%Re-assign arrays
%and display as required (both images taken to be of the same
size). figure(1), imshow(I2_C); figure(2), imshow(I3_C);
%Extract RGB components of the images converting the covertext
into
%normalised floating point form and compute the size of the
arrays. I2_R =I2_C(:, :, 1); I2_G =I2_C(:, :, 2); I2_B
=I2_C(:, :, 3);
I3_R =I3_C(:, :, 1); I3_G =I3_C(:, :, 2); I3_B =I3_C(:, :,
3);
I2_R=im2double(I2_R); I2_G=im2double(I2_G);
I2_B=im2double(I2_B); [N,M]=size(I2_R); %Recover the hidden
(encrypted) data, I1_R=Recover_Data(I2_R,I3_R);
I1_G=Recover_Data(I2_G,I3_G); I1_B=Recover_Data(I2_B,I3_B);
%and regenerate RGB keys
[Key_R,Key_G,Key_B]=Key_Generation(I2_R,I2_G,I2_B);
%Decrypt data by application of Inverse Stochastic Diffusion
ISD_R=Inverse_Stochastic_Diffusion(I1_R,N,M,Key_R);
ISD_G=Inverse_Stochastic_Diffusion(I1_G,N,M,Key_G);
ISD_B=Inverse_Stochastic_Diffusion(I1_B,N,M,Key_B);
%Apply inverse image diffusion process I1_R =
Inverse_Image_Diffusion(ISD_R,I2_R); I1_G =
Inverse_Image_Diffusion(ISD_G,I2_G); I1_B =
Inverse_Image_Diffusion(ISD_B,I2_B);
%Combine RGB components to reconstruct the hidden (colour)
%image and display the result as required and write to file.
J = cat(3,I1_R,I1_G,I1_B); figure(3), imshow(J);
imwrite(J,'Decrypt.bmp','bmp');
```

C.3 Common Functions

```
function [ID] = Image_Diffusion(I1,I2,N,M)
%Function to diffuse one image with another of the same size.
%Transform to Fourier space and compute the power spectrum P.
I1=fft2(I1); I2=fft2(I2); P=abs(I2).^2;
%Check to see if the power spectrum includes a 0, and,
%if so, set value of the power spectrum to 1.
for i=1:N for j=1:M temp=P(i,j); if temp==0 P(i,j)=1; else
      P(i,j)=P(i,j);end  end
end %Filter
data.
ID=I2.*I1./P; %and Inverse Fourier transform, computing the
%real part of the data and normalise the result to give output.
ID=real(ifft2(ID)); ID=ID./max(max(ID));
```

```
function [I1] = Inverse_Image_Diffusion(ISD,I2)
%Transform the input data in to Fourier space. ISD=fft2(ISD);
I2=fft2(I2);
%Filter the data, apply inverse transformation,
%taking the real part and normalise output. I1=conj(I2).*ISD;
I1=real(ifft2(I1)); I1=I1./max(max(I1));
```

```
function [SD] = Stochastic_Diffusion(ID,N,M,Key)
%Compute array of random numbers determined by value of Key.
rand('state',Key); s=rand(N,M);
%Transform into Fourier space and compute power spectrum P.
ID=fft2(ID); S=fft2(s); P=abs(S).^2;
%Check to see if power spectrum includes 0 and if so set to
1.
for i=1:N for
      j=1:M
      temp=P(i,
      j); if
      temp==0
```

```
      P(i,j)=1;
      else
      P(i,j)=P(
      i,j);end
      end
end %Filter the data, inverse Fourier transform and normalise.
SD=S.*ID./P; SD=real(ifft2(SD));
SD=SD./max(max(SD));
```

```
function [ISD] = Inverse_Stochastic_Diffusion(I1,N,M,Key)
%Convert input image into Fourier space.
I1=fft2(I1); %and regenerate pseudo-random number array for
key. rand('state',Key); s=rand(N,M); S=fft2(s); %Filter the
data, apply inverse Fourier transform and normalise.
ISD=conj(S).*I1; ISD=real(ifft2(ISD));
ISD=ISD./max(max(ISD));
```

```
function [Key_R,Key_G,Key_B] = Key_Generation(I2_R,I2_G,I2_B)
%Compute RGB keys by summing the arrays of the associated
%RGB components after multiplication by a large number whose
%value determines the order of magnitude of the key length,
%flooring results to nearest integers towards minus infinity.
I2_R=I2_R*1.0e+10; I2_G=I2_G*1.0e+10; I2_B=I2_B*1.0e+10;
Key_R=floor(sqrt(sum(sum(I2_R.*I2_R))));
Key_G=floor(sqrt(sum(sum(I2_G.*I2_G))));
Key_B=floor(sqrt(sum(sum(I2_B.*I2_B))));
```

```
function [I3] = Hide_Data(I2,SD,c)
%Hide encrypted image SD in covertext image I2 using Fourier
%space addition for information embedding coefficient c.
I3=real(ifft2(c*fft2(SD)+fft2(I2)));
```

```
 function [I1] = Recover_Data(I2,I3)
%Subtract Fourier transform of covertext from %Fourier
transform of stegotext. I1=real(ifft2(fft2(I3)fft2(I2)));
```

```
function Write_TIFF_Image(I);
%Write image to TIFF file maintaining floating point values.
```

```
%Based on 'Writing an image with floating point values',
%Stackoverflow available at
%https://stackoverflow.com/questions/ %14003402/writing-an-
image-with-floating-pointvalues/33353930 t =
Tiff('Stegotext.tif','w'); t.setTag('Photometric',
Tiff.Photometric.RGB);
t.setTag('BitsPerSample', 64); t.setTag('SamplesPerPixel',
3); tagstruct.RowsPerStrip = 16;
t.setTag('SampleFormat',Tiff.SampleFormat.IEEEFP);
t.setTag('ImageLength',size(I,1)); t.setTag('ImageWidth',
size(I,2));
t.setTag('PlanarConfiguration',
Tiff.PlanarConfiguration.Chunky); tagstruct.Software =
'MATLAB'; t.setTag(tagstruct); t.write(I); t.close();
```

Appendix D

PROTOTYPE MATLAB CODE FOR COVERTEXT EXCHANGE

D.1 Function to Phase-Only Encrypt a Colour Images

```
function []=POE(key_R,key_G,key_B)
%FUNCTION: Phase-only Encryption (POD) for full colour images
%INPUTS
%Plaintext colour image
%Key_R: Key for Red component cipher;
%Key_G: Key for Green component cipher;
%Key_B: Key for Blue component cipher;
%c: Spectral Embedding Coefficient set to c=12345.6789
%OUTPUTS
%Three .txt files of ciphertexts.
%Read plaintext colour image (assumed to be a .bmp file) %and
show input image in figure using function 'imshow' %(as
required by the user). I_C=imread('Plaintext.bmp'); figure(1),
imshow(I_C);
%Extract RGB components of the input colour image,
%evaluate image size and convert RGB arrays to floating %point
form (double) - arrays taken to have N rows and M columns.
I_R =I_C(:, :, 1); I_G =I_C(:, :, 2); I_B =I_C(:, :, 3);
[N,M]=size(I_R);
I_R=im2double(I_R); I_G=im2double(I_G); I_B=im2double(I_B);
%Compute the following:
%(i) Uniformly distributed phase arrays for each RGB component
%using the input keys and function 'rand' based on the
%'twister' algorithm. rng(key_R,'twister');
Theta_R=rand(N,M); rng(key_G,'twister'); Theta_G=rand(N,M);
rng(key_B,'twister'); Theta_B=rand(N,M); %(ii) The two-
dimensional DFT of each array using
%function 'fft2', the phase angles (inverse tangent in %radians
between -pi and +pi) associated with real and
```

```
%imaginary components of spectrum using function ’angle’ %and
the phase-only spectra N_R, N_G & N_B.
N_R=exp(i*angle(fft2(Theta_R)));
N_G=exp(i*angle(fft2(Theta_G)));
N_B=exp(i*angle(fft2(Theta_B)));
%Encrypt input RGB components using phase only ciphers
%generated above by taking the DFT of the colour components,
%adding the results to the phase only cipher scaled by the
%embedding coefficient c
I_R=real(ifft2((fft2(I_R).*N_R)+c*N_R));
I_G=real(ifft2((fft2(I_G).*N_G)+c*N_G));
I_B=real(ifft2((fft2(I_B).*N_B)+c*N_B));
%Output the RGB components of the ciphertext (as floating
%point matrices with a precision set to 32-bits to three %.txt
files, each containing the respective component array.
dlmwrite(’R_Enc.txt’,I_R,’delimiter’,’ ’, ’precision’,32);
dlmwrite(’G_Enc.txt’,I_G,’delimiter’,’ ’, ’precision’,32);
dlmwrite(’B_Enc.txt’,I_B,’delimiter’,’ ’, ’precision’,32);
%Cancatenate the RGB component of the ciphertext and show
%normalised output ciphertext image in figure 2 using
%’imshow’ (as required by user). I_R=I_R./max(max(abs(I_R)));
I_G=I_G./max(max(abs(I_G))); I_B=I_B./max(max(abs(I_B))); I_C
= cat(3,I_R,I_G,I_B); figure(2), imshow(I_C);
```

D.2 Function to Phase-Only Decrypt a Colour Image

```
function []=POD(key_R,key_G,key_B)
%FUNCTION: Phase-only Decryption (POD) for full colour images
%INPUTS
%Key_R: Key for Red component cipher;
%Key_G: Key for Green component cipher;
%Key_B: Key for Blue component cipher;
%OUTPUT
%Decrypt colour image (.bmp format).
%Read ciphertext of each RGB encrypted
%component from associated .txt files and compute array size
I_R=dlmread(’R_Enc.txt’); I_G=dlmread(’G_Enc.txt’);
I_B=dlmread(’B_Enc.txt’); [N,M]=size(I_R);
```

```
%Normalise RGB cipherext components to recover colour cipherext
%image I_C and display the result (as required).
I_R_N=I_R./max(max(abs(I_R))); I_G_N=I_G./max(max(abs(I_G)));
I_B_N=I_B./max(max(abs(I_B))); I_C = cat(3,I_R_N,I_G_N,I_B_N);
figure(1), imshow(I_C);
%Re-generate ciphers and phase only spectrum used to encrypt
RGB
%components of the plaitext image using function 'POE'.
rng(key_R,'twister'); Theta_R=rand(N,M);
N_R=exp(i*angle(fft2(Theta_R))); rng(key_G,'twister');
Theta_G=rand(N,M);
N_G=exp(i*angle(fft2(Theta_G))); rng(key_B,'twister');
Theta_B=rand(N,M); N_B=exp(i*angle(fft2(Theta_B)));
%Decrypt the RGB components in Fourier space, apply inverse
DFT
%(using 'ifft2'), take the real components output with
%undefined components being set to zero.
I_R=real(ifft2((fft2(I_R).*conj(N_R)))); I_R(1,1)=0.0;
I_G=real(ifft2((fft2(I_G).*conj(N_G)))); I_G(1,1)=0.0;
I_B=real(ifft2((fft2(I_B).*conj(N_B)))); I_B(1,1)=0.0;
%Concatenate the RGB components to reconstruct a colour
%image, write out decrypt to an image file (assuming .bmp
%format), and show image (as required).
I_C = cat(3,I_R,I_G,I_B); imwrite(I_C,'Decrypt.bmp','bmp');
figure(2), imshow(I_C);
```

Appendix E

PROTOTYPE MATLAB CODE FOR KEY EXCHANGE

E.1 Function for Implementation of a Three-pass Protocol using Phase-only Encryption

```
function []=TPP(key,step,c)

%FUNCTION: Exchange Plaintext composed of an array of
%integers between two
%user - User_1 and User_2 using the Three-pass Protocol
%(TPP) with Phase-only Encryption
%INPUTS
%key: Key(s) used to execute TPP where'key' is a
%string of integer numbers between 0 and 9 with a
%maximum string length of 10 (the limiting upper bound
%for a MATLAB random number generator with a non-negative
%integer seed <2^32) %step:
%step=1 - first pass (first encrypt)
%step=2 - second pass (second encrypt)
%step=3 - third pass (first decrypt)
%step=4 - decryption (second decrypt)
%c: Spectral Embedding Constant c>>1; a user defined for %first
pass only.
%Specification of c is not required for execution of %steps 2,
3 and 4 and the default setting should be 0. Apply step 1 -
first pass.
if step==1
%Read Plaintext P (taken to be an array of       integers
%from 0 to 9) from an ASCII delimited file - Plaintext.txt %-
generated by User_1 to be transferred to User_2.
P=dlmread('Plaintext.txt');
%Zero pad the first element of array due to re-normalisation
%condition which needs to be applied in step 4 when the
```

```
%first element of the decrypt is eliminated from the output.
zero=zeros(1,1); P=[zero P]; N=size(P',1);%Compute size of P.
%Generate cipher using function 'rand' seeded for first user
%defined key. rng(key,'twister'); Theta=rand(1,N);
%Compute phase-only spectrum POS.
POS=exp(i*angle((fft(Theta))));
%Compute phase-only encrypted spectrum E, embed the result %and
return the real component of inverse DFT.
E=(fft(P).*POS)+c*POS;
E=real(ifft(E));
%Write out first pass ciphertext to file which is then sent by
%User_1 to User_2 dlmwrite('Ciphertext.txt',E,'delimiter','
','precision',32); end
%Apply step 2 - second pass. if step==2
%Read first passed ciphertext file %(received
by User_2 from User_1).
E=dlmread('Ciphertext.txt'); N=size(E',1); %Compute size of
array.
%Computer fft of first pass ciphertext. E=fft(E); %Generate
new cipher using function 'rand' seeded by second user
%defined key. rng(key,'twister'); Theta=rand(1,N); %Compute
phase-only encrypted spectrum and return real component
%of inverse DFT. E=E.*exp(i*angle((fft(Theta))));
E=real(ifft(E));
%Write out second pass ciphertext to file which is then sent by
%User_2 to User_1. dlmwrite('Ciphertext.txt',E,'delimiter','
','precision',32); end
%Apply step 3 - third pass. if step==3
%Read second passed ciphertext file %(received
by User_1 from User_2).
E=dlmread('Ciphertext.txt'); N=size(E',1); %Compute size of
array.
%Computer fft of second pass ciphertext. E=fft(E);
%Generate cipher using function 'rand' seeded by
%first user defined key. rng(key,'twister'); Theta=rand(1,N);
%Decrypt phase-only spectrum for first pass and return real
%component of inverse DFT. E=E.*exp(-i*angle((fft(Theta))));
```

```
E=real(ifft(E));
%Write out third pass ciphertext to file which is then sent by
%User_1 to User_2. dlmwrite('Ciphertext.txt',E,'delimiter','
','precision',32); end
%Apply step 4 - Decryption of third pass cipher. if step==4
%Read third pass cipher from file
%(received by User_2 from User_1).
E=dlmread('Ciphertext.txt'); N=size(E',1); %Compute array size.
%Computer fft of second pass cipher.
E=fft(E);
%Generate cipher using function 'rand' seeded by second user
%defined key. rng(key,'twister'); Theta=rand(1,N);
%Decrypt phase-only spectrum for second pass, return
%real component of inverse DFT and re-normalise by
%setting the first element of the %array
to zero.
E=E.*exp(-i*angle((fft(Theta))));
P=real(ifft(E)); P(1)=0.0;
%Convert return to integer values, eliminate first
%element and square
%brackets associated with the array. P=round(P); P(1)=[];
%Write out decrypt to Plaintext.txt file.
dlmwrite('Plaintext.txt',P,'delimiter',' ');
End
```

Appendix F:

16 October 2017

Mrs Philisiwe Joyce Myeza
(942424014) School of Management, IT & **Governance**
Westville Campus

Dear Mrs Myeza,

Protocol reference number: HSS/1752/017D

Project title: User Acceptance of Steganocryptographic methods for archiving and securing academic transcripts

Full Approval

Notification - Expedited Approval In response to your application received on 26 September 2017, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be app!ied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

o,t::: **(Cha;rJ** ....

/ms

Cc Supervisor: Professor Brian McArthur

Cc Academic Leader Research:
Professor Isabel Martins Cc School Administrator: Ms Angela Pearce

---

Humanities & **Social Sciences Research Ethics** Committee

Dr
Shenuka
Singh
(Chair)
Westville
Campus, Govan
Mbeki
Building

Postal **Address:** Private Bag X54001, Durban 4000

Telephone: +27 (0) 31 260 3587/8350/4557 Facsimile: +27 (0) 31 260 4609 Email: ximbap@ukznac.za *I* snymanm@uk.zn.ac.za
mohunp@ykzn.ac.za

Website: WWW ykzn.ac.za

l. 1110 • 20111 I,

100 YEARS OF **ACADEMIC EXCW.ENCE**

FOlff J1r1q C;,·11ourns • Ed!'.18WO()d Howard ColleJie Medical School • Pietermaritzbum • WesMIII!

Appendix G: Qualitative Questionnaires

Questionnaire

To the participant:

Questionnare

Section One (participants: UKZN registrar, examination and records department)

Please tell me what does your job entail? (for all participants)

Does your institution archive academic certificates?

Does your institution archive records of the graduates?

What software is used by your institution to archive the academic certificates or records of the graduates?

How long have you been using the software?

What software was used before this software?

Who is responsible for the technical aspects of the current software?

Who is responsible for the archiving of the data to the software?

Have you ever encountered any difficulties with the software?

If yes, what were those? And how did you solve them?

If no, proceed to the next question

What is working well about the software?

Has there been any unreported and reported illegal activities related to the software?

If yes Please list them, and how were they solved?

If no please proceed to the next question

Please add what you think is relevant to the archiving of academic certificates or graduate records at UKZN that might have not been covered by the questions?

End

Interviewer:

First respondent:

Second respondet:

Third Respondent:

Fourth Respondent:

Fifth Respondent:

Sixth Respondent:

Section Two – the process flow (participants: ICS, examination and records department)

What is your current flow of archiving academic certificates or graduates records at UKZN?

Which server are the records archived to?

Who has the authority to access those archived records?

What technical process is involved in archiving those records e.g. through password etc.

How do you access the archived records when the need arise?

What happened when the person to access archived records is not available?

Who do the system notify when the archived records have been accessed?

How do the system generate the notification that the archived records have been accessed?

Please add what you think is relevant to the process flow that might not have been covered by the questions asked.

End

Interviewer:

First Respondent:

Second Respondent:

Section Three – students (participants: examination and records department)

How do students get to request the certificates if lost etc.?

Who retrieve the information?

What happens if the person suppose to retrieve information is not available?

Please add what you think is relevant to the retrieval of information that might not have been covered by the questions asked

End

Interviewer:

First Respondent:

Second Respondent:

Third Respondent:

Fourth Respondent:

Fifth Respondent:

Section Four Software (Participants: forensic unit, MIE and QVS verification agencies, national qualifications register staff, UKZN auditing firm)

Has the safety features of the archived records been compromised before?

How did you get to know?

How did you solve the problem?

Please add what you think is relevant to the security and safety of the archived records information that might not have been covered by the questions asked.

End

Interviewer:

First Respondent:

Second Respondent:

Third Respondent:

Appendix H

Implementation of steganotechnographic system demonstration questionnaires

ICS Participant

1. demonstrate the process you follow in running the system

2. Is the system easy tointegrate to other university systems
3. Will it be easy to train the end - user of the system
4. What do you see as an advantage and disadvantage of the system at this stage

Could you now train the end user following these questions
Examination and Records participant

1. Please open the system
2. Scan the certificate
3. Archive the certificate
4. Generate the code to use in opening the certificate in the future
5. Open the archived certificate
6. How do you find the process?