The Acceptability of Iris-based Authentication for Public Domain: An Instrumental Design.

Jimoh R. G., Norshuhada Shiratuddin

Graduate Department of Information Technology,
Applied Science Office,
College of Arts and Sciences
Universiti Utara Malaysia
06010, Sintok, Kedah, MALAYSIA
jimoh_rasheed@yahoo.com

ABSTRACT

Innovations in terms of technology have always been a continuous process since change is constant. The invention of information technology has made all services to be rendered in an automated manner. Doing this, the prominent aim is to make all services ubiquitous i.e removing all barriers in terms of time and location, a good example of this is the Automated Teller Machine (ATM) service where banking-related services is rendered in public places for universal access. The beauty of such opportunity is not without its associated security problems with the conventional Personal Identification Number (PIN) entry system. This led to the suggestion of iris-based biometric authentication to guarantee maximum authentication security in all domains. This paper discusses the development of the quantitative instrument (questionnaire) for measuring user's behavioural intention to use iris-based authentication in public places using Unified Theory of Acceptance and Use of Technology (UTAUT) as the underpinning theory. The reliability of the constructs is also discussed.

Keywords
Automated, ubiquitous, iris-base, biometric, authentication.

1.0 INTRODUCTION

In Nigeria, where corruption is at its peak due to series of socio-economic crisis, it has been recommended that the introduction of biometric features for public authentication will go a long way in reducing the corruption level and at the same time resulting into socio-economic growth of the country (Eddy & Akpan, 2008). The author stressed further that there should be inclusion of biometric trait for getting access to banking services via ATM.

It is recently revealed that the victims of ATM unauthorized withdrawals in Nigeria have teamed up and they have sued the central bank of Nigeria (CBN), 24 Nigerian commercial banks and the interswitch (the company responsible for inter connectivity among both Nigerian and international banks to pay a sum of fifty (50) billion naira as the general damages for the withdrawals, 2.5 million naira as the money lost to the withdrawals, 100 million naira as the cost of litigation and lastly 10 million naira as the cost of providing notice to the defendants (Nigerian Tribune, 2009).

Several researchers have proposed iris biometric identification as the alternative to the inherent problems of both token-based (means of identifying an individual based on the evidence of holding a tangible token like identity card) and knowledge-based authentication (means of verifying identify based on having knowledge of something like password) (Jong & Moon, 2007; Hunny, Banshidhar & Phalguni, 2008; Kang & Park, 2009; Dey & Samanta, 2009). It then becomes necessary to determine the acceptance of such authentication technology. This research work has to do with determination of user's acceptance of a more secured, novel approach of authenticating user's identity while using public zone's terminals (iris-based approach) through empirical method. Iris-based authentication is going to be universally considered without being specific about a particular iris processing method. This is to give a universal view based on general characteristics of human iris as a biometric identifier.

2.0 MOTIVATION

The motivation for designing the instrument came from two angles, first, the fact that there are only few studies of technology adoption on public usage (Nataliya, 2004). The second reason for developing a specific instrument is for the fact that previous studies have linked the delay in the implementation of iris authentication to certain constraints like impossibility of working with eye glasses, relatively small distance allowed, wrong positioning, fear eye damage and fear of misuse of the iris image (Searchsecurity.com, 2007; Nataliya, 2004; Desney et al., 2005; Ravirajtech, 2007; Alan et al., 2002; Bandura, 1994). Items added in this respect makes the designed instrument specific for measuring acceptance of iris authentication in public places not even within an organization.

3.0 INSTRUMENT DESIGN

According to Olakunle (2003), it gives the findings of quantitative studies more validity if the items that constitute the instrument are product of research outputs from various points of view in a given domain of study. In line with this, all the items of the questions are evidenced from a number of sources of literature . For the UTAUT constructs, the main items are adapted and reframed to suite this domain of study; other items are from the result of content analysis from previous studies. The development of the main survey instrument in this study is guided by the underpinning theory UTAUT and the relevant literatures. Out of the six dimensions of behavioural intention, Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI) and Facilitating Condition (FC) are contained in the original UTAUT (Venkatesh et al., 2003) where]only Attitude (ATT) and Anxiety (ANX) are the newly included dimensions studies (Taylor & Told, 1995; Davis et al., 1989; Bonnie et al., 2006; Jack et al., 2007; Venkatesh & Davis, 1996; Venkatesh & Davis, 2000; Venkatesh & Morris, 2000). Self-Efficacy (SEF) is also added as an effect variable to establish the correlation between self-efficacy and effort expectancy in this domain of technology diffusion (Bandura, 1994; Venkatesh & Davis; 1996; Jack & Curt, 2007; Venkatesh & Bala, 2008). For every construct in the research instrument, a dummy item is included to discover the seriousness of the respondents in filling the questionnaire so as to determine the usability at individual respondent's level. Table 1 contains the discussion on how the items for each of the constructs are developed. The final instrument is shown in Table 2.

3.1 Performance Expectancy (PE)

This measures the degree to which an individual perceives that using the system could help improve his or her performance. Items under PE are constructed both from the theory, UTAUT and from the relevant literatures. The first four items of the construct, PE1, PE2, PE3 and PE4 are adapted from Venkatesh et al. (2003) and only reframed to suite this domain of study. This is supported with previous related studies (Venkatesh & Davis, 1996; Venkatesh & Davis, 2000; Davis et al., 1989; Venkatesh & Bala, 2008). The fifth item, PE5 is constructed from the view of Nataliya (2004) while the sixth item, PE6 is constructed around a number of studies as well (Daugman, 1993; Anil et al., 2000; Akhilesh & Thomas, 2005; Thomas, 2006; Information Security Magazine, 2007; Ravirajtech, 2007; Jong & Moon, 2007; Manu et al., 2007; Schonberg & Kirovski, 2008). Lastly, the last item in this construct, PE7 is derived from the studies of Alan et al. (2002) and Thomas (2006).

3.2 Effort Expectancy (EE)

This measures the degree to which an individual perceives the system will be easy to use or the degree of associated ease with the use of a system. For the EE construct, a total of five items are constructed for this dimension where all the five items, EE1, EE2, EE3, EE4 and EE5 are equally adapted from venkatesh et al. (2003) and supported by various studies (Venkatesh & Davis, 1996; Venkatesh & Davis, 2000; Davis et al., 1989; Venkatesh & Bala, 2008). The items are similar to that of the conventional perceived ease of use construct of Davis et al. (1998).

3.3 Social Influence (SI)

This measures the degree to which an individual perceives that the person who she cares about feel that she should use the new system. The third dimension of the study, SI construct is made up of six main items where the first three items, SI1, SI2, SI3 and SI4 are adapted from the original UTAUT (Venkatesh et al., 2003) supported by other studies (Bandura, 1994; venkatesh & Morris, 2000). Other items are constructed based on the reviews from various studies in relation to the current issues about the technology under study. For the fifth item SI5, it is constructed around a number of previous studies (Anil et al., 2000; Anil et al., 2008; Nataliya, 2004; Raaavirajtech, 2007). The last item here, SI6 is constructed based on the views of Desney et al. (2005) and Searchsecurity.com (2007).

3.4 Facilitating Condition (FC)

This measure the degree to which an individual believes that an organizational and technical infrastructure is provided to assist in facilitating the use of the system. Considering the six items under FC dimension, similar to the SI construct, the first four items, FAC1, FAC2, FAC3 and FAC4 are adapted from the original UTAUT (Venkatesh et al., 2003) supported by other studies (Bandura, 1994; venkatesh & Morris, 2000). The last two items, FAC5 and FAC6 are constructed around the views of Nataliya (2004) and Alan et al. (2002).

3.5 Attitude (ATT)

Attitudes have been defined within the context of information technology use and acceptance as individual attitudes towards behaviour as to whether to use or accept a new information technology or not (Bonnie, Varun & James, 2006). For the ATT construct, the four items adapted from Venkatesh et al. (2003) are used which are supported by other studies (Taylor & Told, 1995; Davis et al., 1989; Bonnie et al., 2006; Jack et al., 2007).

3.6 Anxiety (ANX)

Individual anxiety towards toward a particular behaviour can be generally defined as the evoking anxious or emotional reactions toward the behaviour in question. The ANX dimension is made up of five survey items, ANX1, ANX2, ANX3, ANX4 and ANX5 which are all adapted from Venkatesh et al. (2003) with evidences from authors of related studies (Venkatesh & Davis, 1996; Venkatesh & Davis, 2000; Venkatesh & Morris, 2000).

3.7 Self-Efficacy (SEF)

According to Bandura (1994), perceived self-efficacy can be defined as the beliefs of people about their capabilities to achieve specified level of performance which plays major role on events that affect their life. The construct SEF is developed from the views of the previous authors who have used the items to measure self-efficacy in various domain of technology diffusion studies. Bandura (1994), Venkatesh and Davis (1996), Jack and Curt (2007) and Venkatesh and Bala (2008) forms the basis of constructing the nine items of the dimension. The importance of the sources is due to the conflicting positions between the studies and Venkatesh et al. (2003) on whether self-efficacy really influence behavioural intention or such influence has been captured by effort expectancy.

3.8 Behavioural Intention (BI) Dimension

This being a standard variable that have been used widely in measuring technology diffusion, the four items of the construct (BI1, BI2, BI3, BI4) are all adapted from Venkatesh et al. (2003) with evidences from authors of related studies (Venkatesh & Davis, 1996; Venkatesh & Davis, 2000; Venkatesh & Morris, 2000).

4.0 MEASURING RELIABILITY

The pilot study which was conducted between February and March, 2009 among 31 ATM users' with 18 males and 13 females. 11 of the respondents falls between age 16 and 30, 12 are between age 31 and 45 while the remaining 8 are above age 45. The reliability testing yields the following results for each of the research variable with a view to justify reliability of the construct through the consistency of its items to measures the variable in question as explained by (Pallant, 2001). As can be seen from the average cronbach's Alpha for all the constructs are greater than 0.7 required with performance expectance (0.882), effort expectancy (0.878), self-efficacy (0.823), attitude (0.909), social influence (0.969), facilitating condition (0.788), anxiety (0.967) and behavioural intention (0.838) as shown in Table1. This means that all the constructs of the instrument are considered reliable as revealed that any reliability of cronbach's alpha of 0.7 and above is acceptable (Sekaran, 2000). It implies that there is consistency among the items that constitute each of the dimensions. This might be attributed to the fact that, the instrument has undergone series of peer review by experts in quantitative studies prior to the pilot study.

Table 1: Average Reliability of the Construct

Construct	No. of items	Average Cronbach's Alpha
Performance Expectancy	7	0.882
Effort Expectancy	5	0.878
Self-efficacy	9	0.823
Attitude	4	0.909
Social Influence	6	0.969
Facilitating Condition	6	0.788
Anxiety	5	0.967
Behavioural Intention	4	0.838

Table 2: Final Instrument items

Items Under Performance expectancy	Code
I would find the technology useful for authentication in public places.	PE1
Using the technology aids in accomplishing authentication more quickly in public places.	PE2
Using the technology will increase my authentication productivity.	PE3
Using the technology will open better opportunities for public transactions without any fear of security threat.	PE4
Using the technology will support the ubiquitous service delivery since nothing external is required for authentication	PE5
Using the technology will facilitate a more secured public authentication.	PE6
Using the technology will help to avoid time wastage.	PE7
Items Under Effort Expectancy	**Code**
If my interaction with the technology would be clear and understandable.	EE1
If it will be useful for me to become skillful at using the technology	EE2
If I find the authentication technology easy to use	EE3
If Learning to operate the technology is easy for me	EE4
If interaction with the system does not require a lot of my mental effort	EE5
Items Under Self-Efficacy	**Code**
If I never use the technology before	SEF1
If I have only the manuals for reference	SEF2
If I could call someone for help if I got stuck	SEF3
If I have seen someone using it before	SEF4
If someone had helped me to get started	SEF5
If a lot of time is given to me	SEF6
If I had got built-in help facility for assistance	SEF7
If someone showed me how to do it first	SEF8
If I have used similar approach before for authentication	SEF9
Items Under Attitude	**Code**
Using the technology is a good idea	ATT1
The technology will make public authentication to be more interesting	ATT2
Working with the technology will be friendly	ATT3
I will like working with the authentication	ATT4

technology	
Items Under Social Influence	**Code**
I am not compelled to use it by people who influence my behaviour	SI1
Using it is not based on the decisions of people who are important to me	SI2
The organization rendering the service will support the use of the authentication technology.	SI3
The authentication device is put in a strategic location	SI4
The fear of the damage the authentication technology can do my eye is removed	SI5
I am sure that my biometric data cannot be misused for unintended purpose at my expense.	SI6
Items Under Facilitating Condition	**Code**
The organization provides all resources required to aid interaction	FAC1
I have the required knowledge to use it	FAC2
The technology is compatible with the previously used one.	FAC3
A specific person is made available in case of difficult situations	FAC4
The authentication technology can work with glasses and lenses	FAC5
The technology can work at a reasonable distance away from the user to avoid the fear of eye damage.	FAC6
Item Under Anxiety	**Code**
There is possibility of feeling apprehensive about using the authentication technology	ANX1
I am likely to be scared of using such complicated technology	ANX2
I hesitate using the technology for fear of making mistakes	ANX3
I considered the technology intimidating	ANX4
I am fully prepared to use the authentication technology as soon as it is fully implemented	ANX5
Items Under Behavioural Intention	**Code**
I intend to use the technology in the nearest future	BI1
I predict I will use the technology as soon as it is fully implemented	BI2
I plan to use the technology in the nearest future	BI3
I intend using the technology provided I have access to it	BI4

5.0 CONCLUSION

The strength of the instrument over the existing technology adoption and diffusion instrument is its ability to integrate the identified constraints behind the successful implementation of the iris authentication technology which makes it to be suitable for the domain and also, it presents technology acceptance in public places which only few studies have contributed in this regard. This paper gives an overview of how the research instrument for measuring acceptability of iris-based authentication through behavioural intention by following both the underpinning theory and the relevant academic literatures and the result of the pilot study shows that the instrument is reliable. The reason for following the due process in the questionnaire development is to validate the contribution that the findings of this is study is going to make both to the theory and practice of technology diffusion most especially in this domain of study. After designing the instrument it is given to five experts in quantitative studies who are senior lecturers and above for proper review before proceeding to pilot testing and more so, the comments resulting from the pilot test are adequately taken care of by making some necessary adjustments to the instrument.

REFERENCES

Akhilesh, C. & Thomas, C. (2005). Challenges and Constraints to the Diffusion of biometrics in Information Systems.*Communication of the ACM, 48*(12), 101 – 106.

Alan, E. Z., Kennethe, A. M. & Kennethe, E. (2002). Comparison of Fingerprint and Iris Biometric Authentication for Control of Digital Signature. *Proceedings of the AMIA 2002 Symposium, pp. 1202.*

Anil, J., Lin, H. & Sharath, P. (2000). Biometric Identification. *Communication of the ACM, 43*(2), 91 -98.

Anil, K. J., Karthik, N. & Abhishek, N. (2008). Biometric Template Security. *EURASIP Journal of Advances in Signal Processing,* 2008,(579416), 1 – 17.

Bandura, A. (1994). Self-Efficacy. Encyclopedia of human behaviour , 2, 71 – 81 from http://www.des.emory.edu/mfp/BanEncy

Bonnie, C. G., Varun, G.& James, T. C. T. (2006). Information System Research with an Attitude. *The Database for Advances in information Systems*, 37(2 & 3).

Daily Newspaper.

Daugman, J. G. (1993) High confidence visual recognition of persons by a test of statistical independence, *IEEE transactions.*

Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35*(8), 982 – 1003.

Desney, S. T., Pedram, K. & Mary, C. (2005). Spy-Resistant Keyboard: More secured Password Entry on Public Touch Screen Displays. *ACM Digital Library, OZCHI 2005 Proceedings.* Page not indicated

Dey, S. & Samanta, D. (2009). An efficient Approach to iris detection for iris biometric processing. *International Journal of Computer Applications in Technology, 35*(1), 2 – 9.

Eddy, E. N. & Akpan, E. E. (2008). Nigerian Government, the public sector and the flight against Corruption: The role of Information and communication *technology. International NGO Journal, 3*(10), 162 – 166.

Hunny, M., Banshidhar, M. & Phaguni, G. (2008). Multi algorithmic Iris Authentication System. *Proceedings of World Academy of Science, Engineering and Technology, 34*, ISSN 2070 – 3740, 148 – 152.

Information Security Magazine. Search Security.com (2007). Retrieved, 2008 from *ww.searchsecurity.techtarget.com/*

Jack, T. M., Chang, L. & Kurt, K. (2007). An Application of the UTAUT Model for Understanding Student Perceptions Using Course Management Software. *Communications of the IIMA, 7*(2), 93 – 104.

Jong, H. P. & Moon, G. K. (2007) Multispecteral Iris Authentication System against Counterfeit attack using gradient-based image fusion. *Society of photo-optical Instrumentation Engineers, 46*.

Kang,P. J. & Park, K. R. (2009) A new multi-unit Iris authentication based on quality assessment and score level fusion for mobile phones. *Machine Visions and Applications.*

Manu, K., Tal, G., Dan, B. and Terry, W.(2007). Reducing Shoulder-Surfing by Using Gaze-based password Entry. *Symposium on Usable Privacy and Security (SOUPS), Pittsburg, USA,* 13 – 19.

Nataliya, B. S. (2004). Access control and Biometrics. *InfosecCd Conference '04*, USA, 124 – 127.

Nigerian Tribune (2009, December 14). Victims of ATM frauds sue CBN, others for N50bn. *Nigerian*

Olakunke, A. O. (2003). *Research Methods in Social Sciences.* (Second Edition),E-Book press, Norway.

Pallant, J. (2001). *A step by step guide to data analysis using SPSS.* Open University Press, McGraw-Hill Education, Philadelphia, USA.

Raviraj Technologies (2007) Iris recognition Biometric Authentication. From *www.ravirajtech.com/iris-recognition-biometric-authentication.html.*

Schonberg, D., & Kirovski, D. (2008). Iris-based biometric identification. *Foreign Patent documents.*

Sekaran, U. (2000). *Research Methods for Business: a skill-buiding approach.* NYC: John Willey Sons, Inc.

Taylor, S., & Todd, P.A. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information System Research 6(*4), 144-176.

Thomas, O. (2006). Keystroke Dynamics: Low Impact Biometric Verification; *http://www.infosecwriter.com/text_resources/pdf/keystroke_tolzak.pdf.* Accessed October 27th, 2008.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science , 45(*2), 186 – 204.

Venkatesh, V., & Bala, H. (2008) Technology Acceptance Model 3and a Research Agenda on Interventions. *Decision Sciences, 39*(2), 273 – 283.

Venkatesh, V., & Davis,F. D.(1996). A Model of Antecedents of Perceived Ease of Use: Development and Test. *Decision Sciences, 27*(3), 451 – 481.

Venkatesh, V., & Morris, M. G. (2000). Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence and their role in Technology Acceptance and Usage Behavior. *MIS Quaterly, 24*(1), 115 – 139.

Venkatesh, V., Morris, M. G., Davis, F. D., & Davis, G. B. (2003). User Acceptance of Information Technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478