UNIVERSITI PUTRA MALAYSIA

DYNAMIC COLOUR TEXT STEGANOGRAPHY MODEL USING RGB CODING AND CHARACTER SPACING TO IMPROVE CAPACITY, INVISIBILITY AND SECURITY

REEMA AHMED ABDALLA BIN THABIT

FSKTM 2022 5

DYNAMIC COLOUR TEXT STEGANOGRAPHY MODEL USING RGB CODING AND CHARACTER SPACING TO IMPROVE CAPACITY, INVISIBILITY AND SECURITY

By

REEMA AHMED ABDALLA BIN THABIT

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

February 2022

DEDICATION

Special for;

My beloved mother,
Fatima Saeed Bin Thabit,

the motivation father,
Ahmed Abdalla Bin Thabit,

the Supportive husband,
Hamada Ahmed Al-Sahoolee,

my lovely kids,
Ahmed, Almass and Ameer,

&

inspirational siblings,
Dr. Nawal, Dr. Walifah, Dr. Huda, Dr. Aqil & Mrs. Hanan

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

DYNAMIC COLOUR TEXT STEGANOGRAPHY MODEL USING RGB CODING AND CHARACTER SPACING TO IMPROVE CAPACITY, INVISIBILITY AND SECURITY

By

REEMA AHMED ABDALLA BIN THABIT

February 2022

Chairman : Associate Professor Ts. Nur Izura binti Udzir, PhD
Faculty : Computer Science and Information Technology

Protecting sensitive information transmitted via public channels is a significant issue faced by governments, militaries, organizations, and individuals. Steganography protects the secret information by concealing it in a transferred object such as video, audio, image, and text. Text is an ideal object for steganography as it uses low bandwidth and is commonly used. Exploit of text features such as font attributes in text steganography has been proposed, however, many existing feature-based text steganography methods suffer from low capacity, weak invisibility and poor security: low capacity is caused by embedding fewer bits per location, utilizing less usable characters, and low compression efficiency; weak invisibility is due to increased colour differences between the cover and the stego text; while poor security resulted from constant mapping and the permanent sequence selection of embedding positions for the hidden message and stego key. To overcome these problems this study proposed the Colour-spacing Text Stego (DCTS) model, which includes four new techniques: a Secret-block & Colour-spacing Matrices Generation (SCMG) technique to achieve high capacity; the Colour Spacing Normalization (CSN) technique to enhance invisibility; and proposed two techniques for two security layers, i.e. the first security layer, the Dynamic Selection of Embedding Positions (DSEP) technique, which hides the secret message and stego key in dynamic positions; and the second security layer, the Dynamic Colour Spacing Mapping (DCSM), which maps the secret message change dynamically. The results of the study found that the DCTS model produces better performance with a high capacity of 98.85% in a small used space by 5.79%, as well as increases the bits per location by 16 bits. Also, it maintains high invisibility by 5.07% when applying black or coloured cover text. With two security layers, the proposed DCTS achieves high security compared to the existing methods. To conclude, the Dynamic Colour-spacing Text Stego-model (DCTS) embeds a high secret data capacity while maintaining invisibility and security. DCTS model offers a

new perspective on feature-based text steganography to protect against visual and statistical attack issues.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

MODEL STEGANOGRAFI TEKS DINAMIK MENGGUNAKAN PENGEKODAN RGB DAN RUANG AKSARA UNTUK MENINGKATKAN KAPASITI, KETIDAKTERLIHATAN DAN KESELAMATAN

Oleh

REEMA AHMED ABDALLA BIN THABIT

Februari 2022

Pengerusi : Profesor Madya Ts. Nur Izura binti Udzir, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Melindungi maklumat sensitif yang dihantar melalui saluran awam adalah isu penting yang dihadapi oleh kerajaan, tentera, organisasi dan individu. Steganografi melindungi maklumat rahsia dengan menyembunyikannya dalam objek yang dipindahkan seperti video, audio, imej dan teks. Teks ialah objek yang ideal untuk steganografi kerana ia menggunakan lebar jalur yang rendah dan biasa digunakan. Eksploitasi ciri teks seperti atribut fon dalam steganografi teks telah dicadangkan, namun banyak kaedah steganografi teks berasaskan ciri sedia ada mengalami kapasiti rendah, ketidakterlihatan lemah dan keselamatan yang lemah: kapasiti rendah disebabkan oleh pembenaman sedikit bit di setiap lokasi, menggunakan aksara yang kurang boleh digunakan, dan kecekapan pemampatan yang rendah; ketidakterlihatan yang lemah adalah disebabkan oleh peningkatan perbezaan warna antara teks pelitup dan teks stego; manakala keselamatan yang lemah terhasil daripada pemetaan berterusan dan pemilihan tetap serta urutan kedudukan benam untuk mesej tersembunyi dan kunci stego. Untuk mengatasi masalah tersebut kajian ini mencadangkan Model Stego Teks Ruang-warna (DCTS) yang merangkumi empat teknik baharu: teknik Penjanaan Matrik Blok-rahsia & Ruang-warna (SCMG) untuk mencapai kapasiti tinggi; teknik Normalisasi Ruang Warna (CSN) untuk meningkatkan ketidakterlihatan; dan mencadangkan dua Teknik untuk keselamatan dua lapisan, iaitu lapisan keselamatan pertama, teknik Pemilihan Dinamik bagi Kedudukan Pembenaman (DSEP), yang menyembunyikan mesej rahsia dan kunci stego dalam kedudukan dinamik; dan lapisan keselamatan kedua, Teknik Pemetaan Warna Ruang Dinamik (DCSM), yang memetakan mesej rahsia berubah secara dinamik. Hasil kajian mendapati model DCTS menghasilkan prestasi yang lebih baik dengan kapasiti tinggi 98.85% dalam ruang terpakai kecil sebanyak 5.79%, serta meningkatkan bit setiap lokasi sebanyak 16 bit. Selain itu, ia mengekalkan ketidakterlihatan tinggi sebanyak 5.07% apabila menggunakan teks penutup hitam atau berwarna. Dengan dua

lapisan keselamatan, DCTS mencapai keselamatan yang tinggi berbanding dengan kaedah sedia ada. Sebagai kesimpulan, model Stego Teks Ruang Warna Dinamik (DCTS) membenamkan data rahsia pada kapasiti yang tinggi sambil mengekalkan ketidakterlihatan dan keselamatan. Model DCTS menawarkan perspektif baharu tentang steganografi teks berasaskan ciri untuk melindungi dari isu serangan visual dan statistik.

ACKNOWLEDGEMENTS

Praise to Almighty Allah for His shower of blessings, I am able to complete this study. I wish to express my sincere and deep gratitude to my supervisor Assoc. Prof Ts. Dr. Nur Izura Udzir and my co-supervisors, Dr. Sharifah Md Yasin and Dr. Aziah Asmawi for their guidance, patience, and support in helping me overcome the various obstacles I faced during my research.

My special gratitude goes to my dearest friends who were always there to motivate each other, extend a helping hand whenever needed, and to share their thoughts despite their own busy schedules and research.

My sweetest appreciation goes to my dearest family, especially my beloved mother and life-coach, for her prayers and my father for his affectionate support and encouragement.

My gratitude to my husband and my lovely kids who accompanied me on the study journey with all its difficulties and success, and they were an encouraging family.

Finally, I wish to thank my siblings and other family members for their understanding and good wishes and constantly helping me to be strong, especially in difficult times.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Nur Izura binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Sharifah bte Md Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Aziah binti Asmawi, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 21 July 2022

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: ______________________ Date: __________________

Name and Matric No: Reema Ahmed Abdalla bin Thabit, GS53053

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ______________________

Name of Chairman of Supervisory Committee: Associate Professor Dr. Nur Izura binti Udzir

Signature: ______________________

Name of Member of Supervisory Committee: Dr. Sharifah bte Md Yasin

Signature: ______________________

Name of Member of Supervisory Committee: Dr. Aziah binti Asmawi

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CSN	Colour & Spacing Normalization
CSct	Colour & Spacing of Cover Text
CSst	Colour & Spacing of Stego Text
CSM	Colour & Spacing Mapping
CT	Cover Text
CSE	Colour & Spacing Extraction
Ccs	cover character size
DCTS	Dynamic Colour-spacing Text Stego
DSEP	Dynamic Selection of Embedding Positions
DCSM	Dynamic Colour & Spacing Mapping
DR	Distortion Robustness
EPst	Embedding Positions of Stego Text
EPct	Embedding of Cover Text
EPstf	First half of EPst
EPsts	Second half of EPst
LSB	Least Significant Bit
LAB	'L' (lightness), 'A' (green / magenta) and 'B' (blue / yellow)
LP	Losing Probability
LCG	Linear Congruential Generator
Nss	normal space size
RGB coding	Red Green Blue coding
Random16	Random of 16 Sequence number array
SM	Secret Message

SK	Stego Key
SB	Secret Block
Skl	stego key location in EPst
Skel	stego key embedding location in ST
SKP	Stego Key Protection
SKE	Stego Key Extraction
SBE	Secret Block Extraction

CHAPTER 1

INTRODUCTION

1.1 Research Background

The rapid expansion of Internet technologies enables the flow of vast amounts of information across the public channel with risks of attacks. Under those circumstances, securing sensitive information has become a serious issue for governments, organizations, and individuals due to the risk of attack. To address this issue, researchers have proposed various methods to protect secure messages transmitted via public and private communication channels.

The two essential methods that play significant roles in information security are data encryption and data hiding. Data encryption is an aspect of cryptography applied to protect the confidentiality of a message being transmitted across private and public channels by converting it to a scribbled enciphered form. Thus, the carrier object after encryption is semantically meaningless. Meanwhile, information hiding conceals the secret message to make it unnoticed/invisible in the course of its transmission via the public (untrusted) communication channel (Din et al., 2018). Invisibility is the fundamental difference between cryptography and information hiding (Ahvanooey et al., 2019).

Information hiding can take one of two forms: watermarking or steganography. Employing watermarking to embed the secret information provides proof of ownership of the carrier object, so it is suitable for copyright protection (Cohen et al., 2018). Steganography, on the other hand, conceals the existence of secret information in the cover carrier (Artz, 2001). Steganography uses several classes of cover media (i.e., audio, video, image, text, network, and DNA).

A text is an “object” utilized by users of the public channel in their daily activities. It is an ideal cover item for data transmitted between a sender and a receiver because of its small size compared to other objects (Khosravi et al., 2019). Moreover, text steganography improves the hiding capacity by exploiting language characteristics, grammatical or orthographic, which differs from one language to another (Aljawarneh et al., 2017; Alsaadi et al., 2018; Kang et al., 2019). Nevertheless, text stenography is one of the most challenged classes of stenography because of the lack of redundant data in text files (Ditta et al., 2018). In addition, text documents have an almost identical structure, which makes changes easily visible.

Social engagements are the most frequent activities of public channel users (Müller, 2020), with 93% of users visiting social networking platforms and 98.1% of users communicating by text. These online activities, which also involve confidential information, present the need for information hiding such as text steganography. At the same time, these activities offer convenient

opportunities and advantages to hide information among the huge availability of online text. For example, social media posts, mail messages, and books in large libraries pose obstacles to eavesdroppers. This is attributed to the difficulty associated with examining, analyzing, and filtering the vast amount of text to determine which text may contain hidden information. In text steganography, the structure and feature characteristics of texts are used to hide secret information.

Text steganography applications use in various domains such as military and intelligence agencies communications (Jia-jia et al., 2018; Karthika et al., 2020; Kumar & Srinivas, 2019; Sadek et al., 2015), banking and finance (Manikandan et al., 2021; Mustafa et al., 2020; Sarkar & Karforma, 2018), (Alrikabi, 2020) , organizations and individuals.

1.2 Problem Statement

The efficiency of text steganography methods are evaluate using four criteria: capacity, invisibility/perceptuality, security and robustness. The current methods suffer from low capacity with weaknesses in invisibility and security against visual and statistical attacks (Alanazi et al., 2021; Khosravi et al., 2019; Mahato et al., 2020; Maji & Mandal, 2020).

Capacity refers to the number of hidden bits in the cover text. The best text steganography hides a large number of secret bits. Nonetheless, the existing methods still suffer from low capacity due to three issues, i.e.:

1. Low number of bits per embedding place (Ahvanooey et al., 2018a; Al-Azzawi, 2018; Al-Nofaie & Gutub, 2020; Aman et al., 2017). Existing text steganography methods hide from one to five bits per location like (Ahvanooey et al., 2018a; Alanazi et al., 2021; Alsaidi et al., 2018; Aman et al., 2017; Khosravi et al., 2019; Kumar et al., 2016a; Mahato et al., 2020; Malik et al., 2017), and others hide from eight to 12 bits in each place, such as (Al-Azzawi, 2018; Naqvi et al., 2018; Osman, 2020; Ramakrishnan et al., 2016).
2. Limited number of usable characters in the cover text (Al-Nofaie & Gutub, 2020; Alanazi et al., 2020, 2021; Ramakrishnan et al., 2016). Although the methods that utilize the font attributes are have more usable characters, they are still limited to alphabet letters only (Osman,

2020; Ramakrishnan et al., 2016) or used limited words based on the part of speech (Al-Azzawi, 2018; Banik & Bandyopadhyay, 2018).

3. Low efficiency of the compression technique which used to reduce the size of secret bits before embedding (Naqvi et al., 2018). The suggested methods in (Malik et al., 2017) applied the LZW compression technique does not produce a short length (Sadié et al., 2020; Xiang et al., 2018a).

Invisibility is related to the unseen existence of hidden messages in the cover text. The excellent text steganography method has high invisibility. However, the existing methods still suffer from weak invisibility caused by two issues:

1. The first issue in invisibility is the stego file is not identical in size to the cover file (Khosravi et al., 2019) by inserting extra characters into the stego text (Ahvanooey et al., 2018a; Alanazi et al., 2020, 2021; Aman et al., 2017; Azeem et al., 2019; Ditta et al., 2018). Hence, size differences can be detected easily by Jaro-Winkler distance (Banik & Bandyopadhyay, 2018; Thabit et al., 2021).
2. The stego text is not identical to the cover text in a colour (Azeem et al., 2019; Khairullah, 2019; Osman, 2020). In (Kumar et al., 2016a; Malik et al., 2017; Sadié et al., 2020), the stego text is generated with rich colour, while (Al-Azzawi, 2018; Osman, 2020) is black, regardless of the cover text colours.

Security points to the protection of the secret message from extraction. Two issues cause poor security against statistical attacks, i.e:

1. Selection of embedding positions and stego key position is sequentially and permanent (Ahvanooey et al., 2018a; Malik et al., 2017; Osman, 2020; Sadié et al., 2020). Although in (Osman, 2020) applies non- sequence embedding, it fails when the secret characters are upsent in the cover text. Besides, in (Al-Azzawi, 2018), the words only are relocated, then the embedding positions are still sequenced in many places.
2. Constant mapping of secret bits in the cover text (Osman, 2020; Ramakrishnan et al., 2016). Most Red, Green, Blue (RGB) coding techniques map the secret bits with pre-defined colours or decimals values as RGB coding (Al-Azzawi, 2018; Malik et al., 2017; Sadié et al., 2020). Despite (Osman, 2020) applying a dynamic mapping, it is restricted to black RGB coding limit from (0,0,0) to (15,15,15) only.
3. The third security issue is protecting the stego key from detection and extraction. Stego key, similar to a cryptography key, comes as a public or private key (Cox et al., 2007). When the key is private, it needs protection from getting it via the public channel during transmission (A. Gutub & K. Alaseri, 2020; Gutub & Alaseri, 2019; Xiong et al., 2019). The researchers in (Ahvanooey et al., 2018a; Osman, 2020; Zneit et

al., 2019), protect the key by hiding it in the cover object. However, their techniques suffer from limitations. In (Ahvanooey et al., 2018a; Zneit et al., 2019), the secret key conceals at the beginning of the cover object for each embedding. Also, in (Osman, 2020), the stego key is hidden before the last character in the cover text. Therefore, the stego key position is known and can be easily attacked by statistical steganalysis. Consequently, obtaining the stego key might extract the hidden message.

Based on what was previously discussed, this study shed light on the existing challenges of capacity, invisibility and security in text steganography methods that utilize the text features. Figure 1.1 displays the summarization of the research problem.

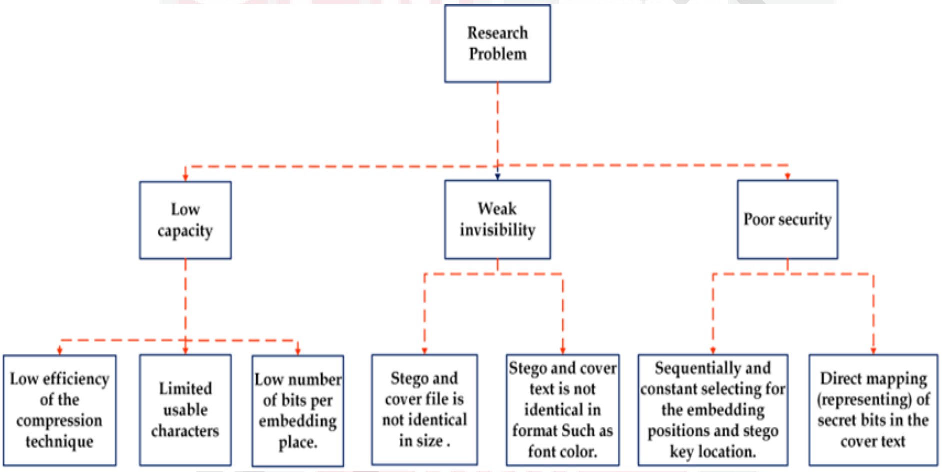

Figure 1.1 : Summarization of research problem

1.3 Research Questions

The central question in this research is concern about how to establish secure communication using text steganography with increased capacity and maintaining invisibility and security. Therefore, the research questions of this study are stated below:

1. How to increase the capacity of text steganography using the font features of text?
2. How to hide the secret message using the RGB coding and character spacing with high invisibility to resist the visual attacks?

3. How to select the embedding positions of the hidden message and stego key in the cover text to enhance security against the statistical attacks?

4. How is the secret message mapped using RGB coding and character spacing to improve the security against the statistical attacks?

1.4 Research Objectives

The main goal of this study is to propose a text stego-model by utilizing the RGB coding and the character spacing with high capacity and maintain the invisibility and security of the hidden message. Hence the objectives of this research are as the following:

1. To propose a text steganography model with high capacity by combining the RGB coding and the character spacing of cover text font.
2. To propose a colour and spacing normalization technique that improves the hidden message's invisibility by reducing the difference between the cover and stego text.
3. To propose a positions selection technique of hidden message and stego key by reordering the positions dynamically to resist the statistical attacks.
4. To propose a dynamic mapping technique of the secret message into the RGB coding and the character spacing, which is more secure against the statistical attacks.

1.5 Research Contributions

The main contribution of this study is a new model of text steganography using RGB coding and colour spacing, named Dynamic Colour-spacing Text Stego (DCTS), which achieves high capacity, enhanced invisibility and improved security. To be more specific, the contributions of this study are as the following:

1. The Secret-block & Colour-spacing Matrices Generation (SCMG) technique increases the capacity by increasing the number of bits per location to carry 16 bits. Besides, it increases the usable characters and compresses the secret message using Huffman coding.
2. The Colour and Spacing Normalization (CSN) technique, which resists hidden message detection against visual attacks by reducing the colour differences between the cover and stego text.
3. The Dynamic Selection of Embedding Positions (DSEP) technique, and Stego Key Protection technique (SKP), the first security layer, to resist the extraction of hidden message and stego key against the

statistical attacks by the non-sequence selection positions hidden message and stego key.

4. The Dynamic Colour and Spacing Mapping (DCSM) technique, the second security layer, to resist the extraction of hidden message against the statistical attacks by changing the mapping of the secret block with the RGB coding and character spacing per embedding.

Table 1.1 exhibits the connection between research problems, research objectives and the contributions of this study.

Table 1.1 : Connections among research problems, objectives and contributions

Research problem	Research objective	Contribution
Low capacity due to the fewer bits per location, the limitation in the number of useable characters, and low efficiency of the use compression technique.	To propose a text steganography model with high capacity by combining the RGB coding and the character spacing of cover text font.	Pre-embedding technique called Secret-block & Colour-spacing Matrices Generation (SGCM) to increase the capacity by reducing the secret message's length using Huffman coding, increased the number of bits per location to carry 16 bits and increased the usable characters by utilising the font attributes.
Weak invisibility against visual attack due to the increased colour difference between the cover and stego text.	To propose a colour and spacing normalization technique that improves the hidden message's invisibility by reducing the difference between the cover and stego text.	Colour and Spacing Normalization (CSN) technique, which resist the hidden message detection against visual attacks.
Poor security of hidden messages and stego key against the statistical attacks by sequentially selecting the embedding places or secret bits.	To propose a positions selection technique of hidden message and stego key by reordering the positions dynamically to resist the statistical attacks.	Dynamic Selection of Embedding Positions (DSEP) technique, and Stego Key Protection technique (SKP), the first security layer, to resist the extraction of hidden message and stego key against the statistical attacks by the non-sequence selection positions hidden message and stego key.
Weak security of hidden messages against the statistical attacks by repeating mapping of the secret block with the RGB coding and character spacing per embedding.	To propose a dynamic mapping technique of the secret message into the RGB coding and the character spacing, which is more secure against the statistical attacks.	Dynamic Colour and Spacing Mapping (DCSM) technique to protect the hidden message against the statistical attacks by changing the mapping of the secret block with the RGB coding and character spacing per embedding.

1.6 Scope of the Study

This study focuses on the feature-based text steganography algorithms that utilizes the RGB coding and character spacing of font text. This study aims to increase the capacity of embedded secret message and maintain invisibility and security against visual and statistical attacks.

Most of the feature-based techniques have limitations in robustness when faced with structural attacks. However, when the usage space ratio is minimized, the number of destroyed places resulting from structural attacks are reduced (Ahvanooey et al., 2018a; Al-Azzawi, 2018; Osman, 2020). Although the DCTS model does not include a new algorithm to enhance its robustness, it shows partial improvement in robustness against structural attacks, such as text format changes in some places of the stego text. The secret blocks in DCTS are hidden in fewer and non-sequential places in the stego text, limiting the possibility of destroying them using structural attacks. Therefore, the DCTS model evaluates and compares the robustness with existing works.

The text in this study is restricted to Latin script, and it also can use the text with black or colour font. The DCTS model can employ the alphabet, number, symbols to hide the secret message into text. The secret message is not limited to text format; it can be an image, video, audio.

1.7 Thesis Organization

This thesis consists of seven chapters. **Chapter 1** presents the introduction of the thesis, including the research problems, research objectives, and contributions of the research.

Chapter 2 has background information on work related to information security and steganography and then narrows down to Feature-based text steganography. The literature review also includes the basics of RGB coding and character spacing techniques in text steganography.

Chapter 3 explains the methodology and process used in the research. It describes the steps taken from the beginning till the final part of the research.

Chapter 4 introduces the proposed design of the Colour and Spacing Text Stego-model. The structure and design of the model consist of two main parts, i.e., Embedding and Extraction Procedures. Embedding Procedure includes five proposed techniques that meet the objectives of this study. Also, it describes the implementation of the proposed Dynamic Colour-spacing Text Stego (DCTS) model and its applicability in various domains.

Chapter 5 presents the results of the analysis section will cover the dissection for the DCTS model tas based on the designed experiments in Chapter 3.

Finally, **Chapter 6** presents the conclusions of the research work carried out in this thesis. In addition, some future directions for exploration are proposed.

1.8 Summary

This chapter contains the thesis's introduction, which includes the research problems, research objectives, and research contributions. Also, it determined the scope of this study.

REFERENCES

Afanasyeva, O. (2015). Analysis of Aspects of Messages Hiding in Text Environments. *Journal of Konbin*, *34*(1), 5.

Agarwal, M. (2013). Text Steganographic Approaches: A Comparison. *International Journal of Network Security & Its Applications (IJNSA)*, *5*(1), 91-106.

Agarwal, N., Singh, A. K., & Singh, P. K. (2019). Survey of Robust and Imperceptible Watermarking. *Multimedia Tools and Applications*, *78*(7), 8603-8633.

Ahvanooey, M. T., Li, Q., Hou, J., Mazraeh, H. D., & Zhang, J. (2018a). AITSteg: An Innovative Text steganography Technique for Hidden Transmission of Text Message via Social Media. *IEEE Access*, *6*, 65981-65995.

Ahvanooey, M. T., Li, Q., Hou, J., Rajput, A. R., & Chen, Y. (2019). Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis. *Entropy*, *21*(4), 355. https://www.mdpi.com/1099-4300/21/4/355

Ahvanooey, M. T., Li, Q., Rabbani, M., & Rajput, A. R. (2017,). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *international journal of advanced computer science and applications*, 30-45. https://doi.org/10.14569/IJACSA.2017.081005

Ahvanooey, M. T., Li, Q., Shim, H. J., & Huang, Y. (2018b). A Comparative Analysis of Information Hiding Techniques for Copyright Protection of Text Documents. *Security and Communication Networks*, *2018*.

Al-Azzawi, A. F. (2018). A Multi-Layer Hybrid Text Steganography for Secret Communication Using Word Tagging and RGB Color Coding. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *10*.

Al-Azzawi, A. F. (2019). A Multi-Layer Arabic Text Steganographic Method Based on Letter Shaping. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *11*.

Al-Nofaie, S., & Gutub, A. (2020). Utilizing Pseudo-spaces to Improve Arabic Text Steganography for Multimedia Data Communications. *Multimedia Tools and Applications*, *79*(1), 19-67. https://doi.org/10.1007/s11042-019-08025-x

Al-Nofaie, S., Gutub, A. A., & Al-Ghamdi, M. (2019). Enhancing Arabic Text Steganography for Personal Usage Utilizing Pseudo-spaces. *Journal of King Saud University-Computer and Information Sciences*.

Alanazi, N., Khan, E., & Gutub, A. (2020). Inclusion of Unicode Standard Seamless Characters to Expand Arabic Text steganography for Secure Individual Uses. *Journal of King Saud University-Computer and Information Sciences*.

Alanazi, N., Khan, E., & Gutub, A. (2021). Efficient Security and Capacity Techniques for Arabic Text Steganography via Engaging Unicode Standard Encoding. *Multimedia Tools and Applications*, *80*(1), 1403-1431. https://doi.org/10.1007/s11042-020-09667-y

Alhaddad, M. J., Alkinani, M. H., Atoum, M. S., & Alarood, A. A. (2020). Evolutionary Detection Accuracy of Secret Data in Audio Steganography for Securing 5G-enabled Internet of Things. *Symmetry*, *12*(12), 2071.

Aljawarneh, S. A., Vangipuram, R., Puligadda, V. K., & Vinjamuri, J. (2017). G-SPAMINE: An Approach to Discover Temporal Association Patterns and Trends in Internet of Things. *Future Generation Computer Systems*, *74*, 430-443.

Alrikabi, H. A. (2020). An Integrity Medical Image Steganography Framework for IoT Based Remote Health Care Applications. *Solid State Technology*, *63*(6), 22343-22358.

Alsaadi, H. I., Al-Anni, M. K., Almuttairi, R. M., Bayat, O., & Ucan, O. N. (2018). Text steganography in Font Color of MS Excel Sheet. Proceedings of the First International Conference on Data Science, E-learning and Information Systems, Madrid, Spain.

AlSabhany, A. A., Ali, A. H., Ridzuan, F., Azni, A., & Mokhtar, M. R. (2020). Digital Audio Steganography: Systematic Review, Classification, and Analysis of the Current State of the Art. *Computer Science Review*, *38*, 100316.

Alsaidi, A., Al-lehaibi, K., Alzahrani, H., AlGhamdi, M., & Gutub, A. (2018). Compression Multi-level Crypto Stego Security of Texts Utilizing Colored Email Forwarding. *Journal of Computer Science & Computational Mathematics (JCSCM)*, *8*(3), 33-42.

Alshahrani, H. M., & Weir, G. (2017). Hybrid Arabic text steganography. *International Journal of Computer and Information Technology*, *6*(6), 329-338.

Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012, November 26–28). *An Introduction to Image Steganography Techniques* 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia.

Aman, M., Khan, A., Ahmad, B., & Kouser, S. (2017). A Hybrid Text Steganography Approach Utilizing Unicode Space Characters and Zero-width Character. *International Journal on Information Technologies and Security*, *9*(1), 85-100.

Anderson, R., & Ross, A. P. (1996, May 30-June). *Information Hiding* First International Workshop on Information Hiding, Cambridge, UK.

Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2019). A Comparative Study of Recent Steganography Techniques for Multiple Image Formats. *International Journal of Computer Network and Information Security*, *11*(1), 11-25.

Artz, D. (2001). Digital Steganography: Hiding Data within Data. *IEEE Internet computing*, *5*(3), 75-80.

Arunkumar, S., Subramaniyaswamy, V., Vijayakumar, V., Chilamkurti, N., & Logesh, R. (2019). SVD-based Robust Image Steganographic Scheme using RIWT and DCT for Secure Transmission of Medical Images. *Measurement*, *139*, 426-437.

Arya, A., & Soni, S. (2018). A literature Review on Various Recent Steganography Techniques. *International Journal on Future Revolution in Computer Science & Communication Engineering*, *4*(1), 143-149.

Aslantas, V. (2008). A Singular-value Decomposition-based Image Watermarking Using Genetic Algorithm. *AEU-International Journal of Electronics and Communications*, *62*(5), 386-394.

Azeem, M., He, J., Rana, K. G., & Rajpoot, F. A. (2019). A Cryptographic Data Hiding Algorithm with High Cover Text Capacity. *International Journal of Electronic Security and Digital Forensics*, *11*, 225-244.

Baawi, S. S., Mokhtar, M., & Sulaiman, R. (2017). New Text Steganography Technique based on a Set of Two-letter Words. *Journal of theoretical and applied information technology*, *95*, 6247-6255.

Bailey, K., Curran, K., & Condell, J. (2004). Evaluation of Pixel-based Steganography and Stegodetection Methods. *The Imaging Science Journal*, *52*(3), 131-150.

Banik, B. G., & Bandyopadhyay, S. (2020). Novel Text Steganography Using Natural Language Processing and Part-of-Speech Tagging. *IETE Journal of Research*, *66*, 384 - 395.

Banik, B. G., & Bandyopadhyay, S. K. (2018). Novel Text Steganography Using Natural Language Processing and Part-of-Speech Tagging. *IETE Journal of Research*, *66*(3), 384-395.

Bedi, P., & Dua, A. (2020, November 5). *Network Steganography Using Extension Headers in IPv6* International Conference on Information, Communication and Computing Technology, Singapore.

Bille, P. (2020). Editorial: Special Issue on Data Compression Algorithms and Their Applications. *Algorithms*, *13*(1), 28. https://www.mdpi.com/1999-4893/13/1/28

Briscoe, S. (2015). Web Searching for Systematic Reviews: A Case Study of Reporting Standards in the UK Health Technology Assessment Programme. *BMC research notes*, *8*(1), 1-7.

Burrows, M., & Wheeler, D. (1994). A Block-sorting Lossless Data Compression Algorithm. Digital SRC Research Report,

Cachin, C. (2004). An Information-theoretic Model for Steganography. *information and computation*, *192*(1), 41-56.

Chandramouli, R. (2002). Mathematical Approach to Steganalysis. Electronic Imaging: Security and Watermarking of Multimedia United States, California, San jose.

Chao, M.-W., Lin, C.-h., Yu, C.-W., & Lee, T.-Y. (2008). A High Capacity 3D Steganography Algorithm. *IEEE transactions on visualization and computer graphics*, *15*(2), 274-284.

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing*, *90*(3), 727-752. https://doi.org/https://doi.org/10.1016/j.sigpro.2009.08.010

Cohen, A., Holmgren, J., Nishimaki, R., Vaikuntanathan, V., & Wichs, D. (2018). Watermarking Cryptographic Capabilities. *SIAM Journal on Computing*, *47*(6), 2157-2202.

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography* (2nd ed.). Morgan kaufmann.

Dai, F. Z., & Cai, Z. (2019). Towards Near-imperceptible Steganographic Text. The 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy.

Devi, K. R., & Prabakaran, S. (2016). An Enhanced Bilateral Information Security towards a Conventional Cryptographic System using DNA Sequences. *Indian Journal of Science and Technology*, *9*(39).

Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on information theory*, *22*(6), 644-654.

Din, R., Samsudin, A., & Lertkrai, P. (2012a). A Framework Components for Natural Language Steganalysis. *International Journal of Computer Theory and Engineering*, *4*(4), 641.

Din, R., Thabit, R., Udzir, N. I., & Utama, S. (2021). Traid-bit Embedding Process on Arabic Text Steganography Method. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 493-500.

Din, R., Tuan Muda, T. Z., Lertkrai, P., Omar, M. N., Amphawan, A., & Aziz, F. A. (2012b, September 24–26). *Text Steganalysis using Evolution Algorithm Approach* 11th WSEAS International Conference on Information Security and Privacy (ISP'12), Prague, Czech Republic.

Din, R., Utama, S., Hanizan, S., Hilal, M. M., Hanif, M., Zulhazlin, A., & Fazali, G. M. (2018). Evaluating the feature-based technique of text steganography based on capacity and time processing parameters. *Advanced Science Letters*, *24*(10), 7355-7359.

Ditta, A., Azeem, M., Naseem, S., Rana, K. G., Khan, M. A., & Iqbal, Z. (2020). A Secure and Size Efficient Algorithm to Enhance Data Hiding Capacity and Security of Cover Text by Using Unicode. *Journal of King Saud University-Computer and Information Sciences*.

Ditta, A., Cai, Y., Azeem, M., Rana, K. G., Yu, H., & Memon, M. Q. (2018). Information Hiding: Arabic Text Steganography by Using Unicode Characters to Hide Secret Data. *International Journal of Electronic Security and Digital Forensics*, *10*, 61-78.

Dulera, S., Jinwala, D., & Dasgupta, A. (2012a). Experimenting with the novel approaches in text steganography. *Int. J. Netw. Secur. Appl*, *3*, 213–225.

Dulera, S., Jinwala, D., & Dasgupta, A. (2012b). Experimenting with the Novel Approaches in Text Steganography. *International Journal of Network Security & Its Applications*, *3*.

Dutta, H., Das, R. K., Nandi, S., & Prasanna, S. M. (2020). An Overview of Digital Audio Steganography. *IETE Technical Review*, *37*(6), 632-650.

Ekodeck, S. G. R., & Ndoundam, R. (2016). PDF Steganography based on Chinese Remainder Theorem. *Journal of Information Security and Applications*, *29*, 1-15.

El Rahman, S. A. (2019). Text Steganography Approaches using Similarity of English Font Styles. *International Journal of Software Innovation (IJSI)*, *7*(3), 29-50.

Festinger, L. (1954). A Theory of Social Comparison Processes. *Human relations*, *7*(2), 117-140.

Fridrich, J., Lisoněk, P., & Soukal, D. (2006). On Steganographic Embedding Efficiency. International Workshop on Information Hiding,

Gaur, M., & Sharma, M. (2015). A New PDAC (parallel encryption with digit arithmetic of cover text) based Text Ssteganography Approach for Cloud Data Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *3*(3), 344-1352.

Girdhar, A., & Kumar, V. (2018). Comprehensive Survey of 3D Image Steganography Techniques. *IET Image Processing*, *12*(1), 1-10.

Gu, J., & Cheng, Y. (2010, April 16-18). A Watermarking Scheme for Natural Language Documents. 2010 2nd IEEE International Conference on Information Management and Engineering, Chengdu, China.

Gutub, A., & Al-Ghamdi, M. (2019). Image based Steganography to Facilitate Improving Counting-based Secret Sharing. *3D Research*, *10*(1), 6.

Gutub, A., & Alaseri, K. (2020). Hiding Shares of Counting-based Secret Sharing via Arabic Text Steganography for Personal Usage. *Arabian Journal for Science and Engineering*, *45*(4), 2433-2458.

Gutub, A. A., & Alaseri, K. (2019). Refining Arabic Text Stego-techniques for Shares Memorization of Counting-based Secret Sharing. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/https://doi.org/10.1016/j.jksuci.2019.06.014

Gutub, A. A., & Alaseri, K. (2020). Hiding Shares of Counting-based Secret Sharing via Arabic text Steganography for Personal Usage. *Arabian Journal for Science and Engineering*, *45*(4), 2433-2458.

Gutub, A. A., & Alaseri, K. (2020). Hiding Shares of Counting-Based Secret Sharing via Arabic Text Steganography for Personal Usage. *Arabian Journal for Science and Engineering*, *45*, 2433-2458.

Hakak, S., Kamsin, A., Tayan, O., Idris, M. Y. I., & Gilkar, G. A. (2019). Approaches for Preserving Content Integrity of Sensitive Online Arabic Content: A Survey and Research Challenges. *Information Processing & Management*, *56*(2), 367-380.

Hamdan, A. M., & Hamarsheh, A. (2016). AH4S: An Algorithm of Text in Text Steganography using the Structure of Omega Network. *Security and Communication Networks*, *9*(18), 6004-6016.

Hamdani, H., Ismanto, H., Munir, A. Q., Rahmani, B., Syafrianto, A., Suprihanto, D., & Septiarini, A. (2018a). The Proposed Development of Prototype with Secret Messages Model in Whatsapp Chat. *International Journal of Electrical & Computer Engineering (2088-8708)*, *8*(5).

Hamdani, H., Ismanto, H., Munir, A. Q., Rahmani, B., Syafrianto, A., Suprihanto, D., & Septiarini, A. (2018b). The Proposed Development of Prototype with Secret Messages Model in Whatsapp Chat. *International Journal of Electrical & Computer Engineering*, *8*(5).

Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image Steganography Techniques: An Overview. *International Journal of Computer Science and Security (IJCSS)*, *6*(3), 168-187.

Hosseini, M. (2012, January 2012). *A Survey of Data Compression Algorithms and their Applications* Applications of Advanced Algorithms, British Columbia, Canada.

Huanhuan, H., Xin, Z., Weiming, Z., & Nenghai, Y. (2017, June 26-29). Adaptive Text Steganography by Exploring Statistical and Linguistical Distortion. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China.

Huffman, D. A. (1952). A Method for the Construction of Minimum-Redundancy Codes. *Proceedings of the IRE*, *40*(9), 1098-1101. https://doi.org/10.1109/JRPROC.1952.273898

Jalil, Z., & Mirza, A. M. (2013). A Robust Zero-watermarking Algorithm for Copyright Protection of Text Documents. *Journal of the Chinese Institute of Engineers*, *36*(2), 180-189.

Jaro, M. A. (1989). Advances in Record-linkage Methodology as Applied to Matching the 1985 census of Tampa, Florida. *Journal of the American Statistical Association*, *84*(406), 414-420.

Jayasankar, U., Thirumal, V., & Ponnurangam, D. (2018). A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. *Journal of King Saud University - Computer and Information Sciences*, *33*(2), 119-140. https://doi.org/https://doi.org/10.1016/j.jksuci.2018.05.006

Jia-jia, J., Xian-quan, W., Fa-jie, D., Xiao, F., Han, Y., & Bo, H. (2018). Bio-inspired steganography for secure underwater acoustic communications. *IEEE Communications Magazine*, *56*(10), 156-162.

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. *Neurocomputing*, *335*, 299-326.

Kang, Y., Liu, F., Yang, C., Luo, X., & Zhang, T. (2019). Color Image Steganalysis based on Residuals of Channel Differences. *Computers, Materials and Continua*, *59*(1), 315-329.

Karthika, P., Babu, R. G., & Jayaram, K. (2020). Biometric based on steganography image security in wireless sensor networks. *Procedia Computer Science*, *167*, 1291-1299.

Kaur, A., Sethi, N., & Singh, H. (2015). A Review on Data Compression Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 1(1).

Kawaguchi, E., & Eason, R. O. (1999). Principles and Applications of BPCS Steganography. Multimedia systems and applications,

Kellen, T. (2001). *Hiding in plain view: Could steganography be a terrorist tool?* GIAC. https://www.sans.org/white-papers/551/

Khairullah, M. (2019). A novel steganography method using transliteration of Bengali text. *Journal of King Saud University-Computer and Information Sciences*, *31*(3), 348-366.

Kharrazi, M., Sencar, H. T., & Memon, N. (2007). Image Steganography and Steganalysis: Concepts and Practice. In *Mathematics And Computation In Imaging Science And Information Processing* (pp. 177-207). World Scientific.

Khosravi, B., Khosravi, B., Khosravi, B., & Nazarkardeh, K. (2019). A new method for pdf steganography in justified texts. *Journal of Information Security and Applications*, *45*, 61-70. https://doi.org/https://doi.org/10.1016/j.jisa.2019.01.003

Korzhik, V., Fedyanin, I., & Cuong, N. D. (2017, April 3–7). *Detection of stegosystems using block ciphers for encryption of the embedded messages* 2017 20th Conference of Open Innovations Association (FRUCT), Saint Petersburg, Russia.

Kour, J., & Verma, D. (2014). Steganography Techniques–A Review Paper. *International Journal of Emerging Research in Management & Technology*, *3*(5), 132-135.

Kumar, A., & Pooja, K. (2010). Steganography-A Data Hiding Technique. *International Journal of Computer Applications*, *9*(7), 19-23.

Kumar, P. M., & Srinivas, K. (2019, Nov. 27-29). *Real Time Implementation of Speech Steganography* 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India.

Kumar, R., Chand, S., & Singh, S. (2015). An efficient text steganography scheme using Unicode Space Characters. *International Journal of Forensic Computer Science*, *10*(1), 8-14.

Kumar, R., Malik, A., Singh, S., & Chand, S. (2016a, Feb. 11-12). *A high capacity email based text steganography scheme using Huffman compression* 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India.

Kumar, R., Malik, A., Singh, S., Kumar, B., & Chand, S. (2016b, April 29-30). *A space based reversible high capacity text steganography scheme using font type and style* 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India.

Kuniavsky, M. (2003). Observing the User Experience: a Practitioner's Guide to User Research. USA: Morgan Kaufmann

Langdon, G. G. (1984). An introduction to arithmetic coding. *IBM Journal of research and development*, *28*(2), 135-149.

Lee, C.-F., & Chen, H.-L. (2013). Lossless Text Steganography in Compression Coding. In *Recent Advances in Information Hiding and Applications* (pp. 155-179). Springer: Berlin/Heidelberg, Germany. https://doi.org/10.1007/978-3-642-28580-6_8

Li, N., Hu, J., Sun, R., Wang, S., & Luo, Z. (2017). A High-Capacity 3D Steganography Algorithm With Adjustable Distortion. *IEEE Access*, *5*, 24457-24466.

Liao, X., Yin, J., Chen, M., & Qin, Z. (2020). Adaptive Payload Distribution in Multiple Images Steganography based on Image Texture Features. *IEEE Transactions on Dependable and Secure Computing*.

Liu, J.-W., Lu, T.-C., & Zhao, Q. (2017, November 8–10). *Improving the performance of lossless reversible steganography via data sharing* 2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST), Taichung, Taiwan.

Liu, T., & Tsai, W. (2007). A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique. *IEEE Transactions on Information Forensics and Security*, *2*(1), 24-30. https://doi.org/10.1109/TIFS.2006.890310

Liu, Y., Liu, S., Wang, Y., Zhao, H., & Liu, S. (2019). Video Steganography: A Review. *Neurocomputing*, *335*, 238-250.

Loukhaoukha, K., Nabti, M., & Zebbiche, K. (2014). A robust SVD-based image watermarking using a multi-objective particle swarm optimization. *Opto-Electronics Review*, *22*(1), 45-54.

Mahato, S., Khan, D., & Yadav, D. K. (2020). A modified approach to data hiding in Microsoft Word documents by change-tracking technique. *Journal of King Saud University - Computer and Information Sciences*, *32*, 216-224.

Mahato, S., Yadav, D. K., & Khan, D. (2013, June). A Novel Approach to Text Steganography Using Font Size of Invisible Space Characters in Microsoft Word Document. Proceedings of the International Conference on Advanced Computing, Networking, and Informatics, New Delhi, India.

Maji, G., & Mandal, S. (2020). A forward email based high capacity text steganography technique using a randomized and indexed word dictionary. *Multimedia Tools and Applications*, *79*(35), 26549-26569. https://doi.org/10.1007/s11042-020-09329-z

Malathi, P., Manoaj, M., Manoj, R., Raghavan, V., & Vinodhini, R. (2017). Highly Improved DNA based Steganography. *Procedia Computer Science*, *115*, 651-659.

Malik, A., Sikka, G., & Verma, H. K. (2017). A High Capacity Text Steganography Scheme based on LZW Compression and Color Coding. *Engineering Science and Technology, an International Journal*, *20*(1), 72-79.

Manikandan, T., Muruganandham, A., Babuji, R., Nandalal, V., & Iqbal, J. M. (2021, April 23). Secure E-Health using Images Steganography. National Virtual Conference on Advanced Informatics, Electronics and Vision 2021 (NCAIEV'21), Pollachi, India.

Mansor, F. Z., Mustapha, A., & Samsudin, N. A. (2017, May 6–7). Researcher's perspective of substitution method on text steganography. IOP Conference Series: Materials Science and Engineering, Melaka, Malaysia.

Marsaglia, G. (1972). The structure of linear congruential sequences. In *Applications of Number Theory to Numerical Analysis* (pp. 249-285). Elsevier.

Mishra, S., Yadav, V. K., Trivedi, M. C., & Shrimali, T. (2018). Audio Steganography Techniques: A survey. In *Advances in Computer and Computational Sciences* (pp. 581-589). Springer.

Mokrzycki, W., & Tatol, M. (2011). Colour difference∆ E-A survey. *Machine Graphics and Vision*, *20*(4), 383-411.

Mollin, R. A. (2006). *An Introduction to Cryptography* (2nd ed.). Chapman and Hall/CRC. https://doi.org/https://doi.org/10.1201/9781420011241

Montanari, A. (2018). *EE 388 – Modern Coding Theory*. Stanford University, Spring https://web.stanford.edu/class/ee388/

Morgado, F. (2017). Character Attributes. In F. Morgado (Ed.), *Microsoft Word Secrets: The Why and How of Getting Word to Do What You Want* (pp. 95-148). Apress. https://doi.org/10.1007/978-1-4842-3078-7_3

Mstafa, R. J., Younis, Y. M., Hussein, H. I., & Atto, M. (2020). A New Video Steganography Scheme based on Shi-Tomasi Corner Detector. *IEEE Access*, *8*, 161825-161837.

Müller, J. (2020). *Online Activities of Internet Users in Malaysia of May 2020*. Retrieved 24 April 2021 from https://www.statista.com/statistics/788504/online-activities-of-internet-users-by-activity-malaysia/

Mustafa, S., Rahim, M. S. M., Ahmed, F. Y., & Mahdi, M. (2020). Hiding Financial Data In Bank Card Image Using Contrast Level Value And Text Encryption For Worthiness A Robust Steganography Method. *International Journal of Advanced Science and Technology*, *29*, 2783-2801.

Nagarhalli, T. P., & Save, A. M. (2017, March 17-18). *A cross lingual technique for hiding Hindi text* 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India.

Naqvi, N., Abbasi, A. T., Hussain, R., Khan, M. A., & Ahmad, B. (2018). Multilayer partially homomorphic encryption text steganography (MLPHE-TS): a zero steganography approach. *Wireless Personal Communications*, *103*(2), 1563-1585.

Nazari, M., & Ahmadi, I. D. (2020). A Novel Chaotic Steganography Method with Three Approaches for Color and Grayscale Images based on FIS and DCT with Flexible Capacity. *Multimedia Tools and Applications*, *79*(19), 13693-13724.

Nelson, M. (1996). Data compression with the Burrows-Wheeler transform. *Dr. Dobb's Journal*.

Notes, D. L. (2012). compression Algorithms: Huffman and Lempel-Ziv-Welch (Lzw). *Last Update: February*, *13*.

Obeidat, A. A. (2017). Arabic Text Steganography Using Unicode of Non-Joined to Right Side Letters. *Journal of Computational Science*, *13*(6), 184-191.

Odeh, A., Elleithy, K., & Faezipour, M. (2014, April 3-5). Steganography in text by using MS word symbols. Proceedings of the 2014 Zone 1 Conference of the American Society for Engineering Education, Bridgeport, CT, USA.

Osman, B. (2020). *Message Hiding Technique in Text Steganography using RGB Colour Approach and Random Location* [Unpublished doctoral dissertation, Universiti Utara Malaysia]. Changlun, Malaysia.

Osman, B., Yasin, A., & Omar, M. N. (2016). An Analysis of Alphabet-based Techniques in Text Steganography. *Journal of Telecommunication, Electronic and Computer Engineering*, *8*(10), 109-115.

Pandya, I., Jhajj, S., & Pawar, R. (2017, September 13–16). *A steganographic approach to mitigate password attacks* 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Manipal, India.

Pasco, R. (1977). Source coding algorithms for fast data compression *IEEE Transactions on information theory*, *23*(4), 548-548. https://doi.org/10.1109/TIT.1977.1055739

Patel, I., & Goud, J. (2012). Colour recognition for blind and colour blind people. *International Journal of Engineering and Technology Innovation*, *2*(6), 38-42.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062-1078.

Por, L. Y., & Delina, B. (2008, April 6-8). Information Hiding: A New Approach in Text Steganography. 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China.

Prabakaran, G., Bhavani, R., & Rajeswari, P. (2013, March 20–21). *Multi secure and robustness for medical image based steganography scheme* 2013 international conference on circuits, power and computing technologies (ICCPCT), Nagercoil, India.

Rachmawanto, E. H. (2019). An improved security and message capacity using AES and Huffman coding on image steganography. *TELKOMNIKA*, *17*(5), 2400-2409.

Rahman, M., & Hamada, M. (2020). Burrows–Wheeler Transform Based Lossless Text Compression Using Keys and Huffman Coding. *Symmetry*, *12*(10), 1654.

Rahman, M. S., Khalil, I., & Yi, X. (2019). A lossless DNA data hiding approach for data authenticity in mobile cloud based healthcare systems. *International Journal of Information Management*, *45*, 276-288.

Ramakrishnan, B. K., Thandra, P. K., & Srinivasula, A. S. M. (2016). Text Steganography: A Novel Character-level Embedding Algorithm using Font Attribute. *Security and Communication Networks*, *9*(18), 6066-6079.

Richardson, T., & Urbanke, R. (2008). *Modern Coding Theory*. Cambridge University Press.

Rissanen, J., & Langdon, G. G. (1979). Arithmetic coding. *IBM Journal of research and development*, *23*(2), 149-162.

Roslan, N. A., Mahmod, R., Udzir, N. I., & Zurkarnain, Z. A. (2014). Primitive Structural Method for High Capacity Text Steganography. *Journal of Theoretical & Applied Information Technology*, *67*(2).

Roslan, N. A., Udzir, N. I., Mahmod, R., Zukarnain, Z. A., Ninggal, M. I. H., & Thabit, R. (2020). Character Property Method for Arabic Text Steganography with Biometric Multifactor Authentication Using Liveness Detection. *Journal of Theoretical & Applied Information Technology*, *98*, 4140-4157.

Sabeti, V., & Shoaei, M. (2020). New High Secure Network Steganography Method Based on Packet Length. *The ISC International Journal of Information Security*, *12*(1), 24-44.

Sabri, R. S., Din, R., & Mustapha, A. (2018). Analysis Review on Performance Metrics for Extraction Schemes in Text Steganography. *Indonesian Journal of Electrical Engineering and Computer Science*.

Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. (2015). Video steganography: a comprehensive review. *Multimedia Tools and Applications*, *74*(17), 7063-7094.

Sadié, J. K., Metcheka, L. M., & Ndoundam, R. (2020). Two High Capacity Text Steganography Schemes Based on Color Coding. *arXiv preprint arXiv:2004.00948*, *3*.

Salton, G. (1989). Automatic Text Processing: The Transformation, Analysis, and Retrieval of Information by Computer. *Addison-Wesley*, *169*.

Sarkar, A., & Karforma, S. (2018). Image Steganography Using Password Based Encryption Technique to Secure E-banking Data. *International Journal of Applied Engineering Research*, *13*(22), 15477-15483.

Sasi, S. B., & Sivanandam, N. (2015). A Survey on Cryptography Using Optimization Algorithms in WSNs. *Indian Journal of Science and Technology*, *8*(3), 216.

Satir, E., & Isik, H. (2014). A Huffman compression based text steganography method. *Multimedia Tools Appl.*, *70*(3), 2085–2110. https://doi.org/10.1007/s11042-012-1223-9

Satir, E., & Isik, H. (2014). A Huffman Compression Based Text Steganography Method. *Multimedia Tools and Applications*, *70*(3), 2085-2110.

Setyaningsih, E., Wardoyo, R., & Sari, A. K. (2020). Securing Color Image Transmission Using Compression-encryption Model with Dynamic Key Generator and Efficient Symmetric Key Distribution. *Digital Communications and Networks*, *6*(4), 486-503.

Shah, P. D., & Bichkar, R. S. (2018). *A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator* International Conference on Intelligent Computing and Applications, Springer, Singapore.

Shah, S. T. A., Khan, A., & Hussain, A. (2020). Text Steganography Using character Spacing after Normalization. *International Journal of Scientific & Engineering Research*, *11*(2).

Shaker, A. A., Ridzuan, F., & Pitchay, S. A. (2017). Text Steganography Using Extensions Kashida Based on the Moon and Sun Letters Concept. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(8), 286-290.

Shannon, C. E. (1949). Communication in the Presence of Noise. *Proceedings of the IRE*, *37*(1), 10-21.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *The Bell system technical journal*, *28*(4), 656-715.

Shiu, H. J., Lin, B. S., Lin, B. S., Huang, P. Y., Huang, C. H., & Lei, C. L. (2017, September19–21). Hiding on Social Media Communications Using Text Steganography. International Conference on Risks and Security of Internet and Systems, Dinard, France.

Shoba, D. J., & Sivakumar, S. (2017). A Study on Data Compression Using Huffman Coding Algorithms. *International Journal of Computer Science Trends and Technology (IJCST)*, *5*(1), 58-63.

Shutko, N., Urbanovich, P., & Zukowski, P. (2018). A Method of Syntactic Text steganography based on Modification of the Document-container Aprosh. *Przeglad Elektrotechniczny*.

Simmons, G. J. (1984). The Prisoners' problem and the Subliminal Channel. In D. E. Chaum (Ed.), *Advances in Cryptology* (pp. 51-67). Springer, Boston. https://doi.org/10.1007/978-1-4684-4730-9_5

Singh, A., & Singh, G. (2014). A Survey on Different text Data Compression Techniques. *International Journal of Science and Research (IJSR)*.

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*.

Suen, C. Y., Dumont, N., Dyson, M., Tai, Y.-C., & Lu, X. (2011, Sept 18-21). *Evaluation of Fonts for Digital Publishing and Display* 2011 International Conference on Document Analysis and Recognition, Beijing, China.

Taha, A., Hammad, A. S., & Selim, M. M. (2018). A High Capacity Algorithm for Information Hiding in Arabic Text. *Journal of King Saud University-Computer and Information Sciences*, *32*(6), 658-665.

Tancik, M., Mildenhall, B., & Ng, R. (2020). Stegastamp: Invisible Hyperlinks in Physical Photographs. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,

Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., Roslan, N. A., & Din, R. (2021). A Comparative Analysis of Arabic Text Steganography. *Applied Sciences*, *11*(15), 6851.

Uthayakumar, J., Vengattaraman, T., & Dhavachelvan, P. (2018). A Survey on Data Compression Techniques: From the Perspective of Data Quality, Coding Schemes, Data Type and Applications. *Journal of King Saud University-Computer and Information Sciences*.

Vaishakh, K., Pravalika, A., Abhishek, D., Meghana, N., & Prasad, G. (2019, November 4). A Semantic Approach to Text Steganography in Sanskrit Using Numerical Encoding.*Advances in Intelligent Systems and Computing* Recent Findings in Intelligent Computing Techniques Springer, Singapore.

Verdu, S. (1998). Fifty Years of Shannon Theory. *IEEE Transactions on information theory*, *44*(6), 2057-2078.

Vidhya, P. M., & Paul, V. (2015). Unicode-based method for text steganography with malayalam text. *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology*, *28*(4), 1591–1600.

Vijayakumar, P., Vijayalakshmi, V., & Rajashree, R. (2018). Increased Level of Security using DNA Steganography. *International Journal of Advanced Intelligence Paradigms*, *10*(1-2), 74-82.

Walia, E., Jain, P., & Navdeep, N. (2010). An Analysis of LSB & DCT based Steganography. *Global Journal of Computer Science and Technology*.