AN IMPROVED IMAGE STEGANOGRAPHY SCHEME BASED ON DISTINCTION GRADE VALUE AND SECRET MESSAGE ENCRYPTION

MUSTAFA SABAH TAHA

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

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

OCTOBER 2020

DEDICATION

To the prophet of mercy “Muhammad bin Abdullah (Peace Be Upon Him)”
and my beloved country (Iraq).

ACKNOWLEDGEMENT

First and foremost, all praise and thanks are due to Allah, and peace and blessings be upon his Messenger, Mohammed (Peace Be Upon Him). Next, I wish to express my sincere appreciation to my main supervisor, Prof. Dr. Mohd Shafry Mohd Rahim. for encouragement, guidance, critics, and friendship. I indeed thank him for showing me how to identify interesting problems and how the research can be started and finished correctly.

In preparing this thesis, I got engaged with many researchers, academics and practitioners. Thus, I want to thank those especially Dr. Maznah Kamat, who have contributed to my understanding and thoughts. I also want to express my sincere appreciation to all my UTM colleagues for their support and encouragement in accomplishing this work. Their views and tips were really helpful.

Finally, I am grateful to all my family members for their support and dua'a. In particular, I would like to thank my wife for her patience, encouragement, support and understanding.

ABSTRACT

Steganography is an emerging and greatly demanding technique for secure information communication over the internet using a secret cover object. It can be used for a wide range of applications such as safe circulation of secret data in intelligence, industry, health care, habitat, online voting, mobile banking and military. Commonly, digital images are used as covers for the steganography owing to their redundancy in the representation, making them hidden to the intruders, hackers, adversaries, unauthorized users. Still, any steganography system launched over the Internet can be cracked upon recognizing the stego cover. Thus, the undetectability that involves data imperceptibility or concealment and security is the significant trait of any steganography system. Presently, the design and development of an effective image steganography system are facing several challenges including low capacity, poor robustness and imperceptibility. To surmount such limitations, it is important to improve the capacity and security of the steganography system while maintaining a high signal-to-noise ratio (PSNR). Based on these factors, this study is aimed to design and develop a distinction grade value (DGV) method to effectively embed the secret data into a cover image for achieving a robust steganography scheme. The design and implementation of the proposed scheme involved three phases. First, a new encryption method called the shuffle the segments of secret message (SSSM) was incorporated with an enhanced Huffman compression algorithm to improve the text security and payload capacity of the scheme. Second, the Fibonacci-based image transformation decomposition method was used to extend the pixel's bit from 8 to 12 for improving the robustness of the scheme. Third, an improved embedding method was utilized by integrating a random block/pixel selection with the DGV and implicit secret key generation for enhancing the imperceptibility of the scheme. The performance of the proposed scheme was assessed experimentally to determine the imperceptibility, security, robustness and capacity. The standard USC-SIPI images dataset were used as the benchmarking for the performance evaluation and comparison of the proposed scheme with the previous works. The resistance of the proposed scheme was tested against the statistical, χ^2, Histogram and non-structural steganalysis detection attacks. The obtained PSNR values revealed the accomplishment of higher imperceptibility and security by the proposed DGV scheme while a higher capacity compared to previous works. In short, the proposed steganography scheme outperformed the commercially available data hiding schemes, thereby resolved the existing issues.

ABSTRAK

Steganografi adalah teknik baru muncul dan sangat diperlukan untuk komunikasi maklumat yang selamat melalui internet menggunakan objek penutup rahsia. Ia boleh digunakan untuk pelbagai aplikasi seperti edaran data rahsia yang selamat dalam perisikan, industri, penjagaan kesihatan, habitat, undian atas talian, perbankan mudah alih dan ketenteraan. Biasanya, imej digital digunakan sebagai penutup untuk steganografi disebabkan oleh kelebihannya dalam perwakilan, menjadikan ia tersembunyi daripada penceroboh, penggodam, musuh, pengguna yang tidak dibenarkan. Namun, setiap sistem steganografi yang dilancarkan melalui Internet dapat dipecahkan apabila penutup stego itu dikenali. Oleh itu, keberkesanan yang melibatkan ketidaklihatan data atau penyembunyian dan keselamatan adalah ciri penting bagi setiap sistem steganografi. Pada masa kini, reka bentuk dan pembangunan sistem steganografi imej yang berkesan menghadapi beberapa cabaran termasuk kapasiti yang rendah, keteguhan dan ketidaklihatan yang lemah. Untuk mengatasi keterbatasan ini, adalah penting untuk meningkatkan keupayaan dan keselamatan sistem steganografi sambil mengekalkan nisbah isyarat-kepada-hingar (PSNR) yang tinggi. Berdasarkan faktor-faktor ini, kajian ini bertujuan untuk mereka bentuk dan membangunkan kaedah nilai gred perbezaan (DGV) untuk membenamkan data rahsia secara berkesan ke dalam imej penutup untuk mencapai skema steganografi yang mantap. Reka bentuk dan pelaksanaan skim yang dicadangkan ini melibatkan tiga fasa. Pertama, kaedah penyulitan baharu yang dikenali sebagai merombak segmen mesej rahsia (SSSM) digabungkan dengan algoritma pemampatan Huffman yang dipertingkatkan untuk meningkatkan keselamatan teks dan keupayaan muatan pada skim ini. Kedua, kaedah penguraian transformasi imej berasaskan Fibonacci digunakan untuk memanjangkan bit piksel dari 8 kepada 12 untuk meningkatkan keteguhan skim ini. Ketiga, kaedah pembenaman yang ditambahbaik digunakan dengan mengintegrasikan pilihan blok/piksel secara rawak dengan DGV dan penjanaan kunci rahsia tersirat untuk meningkatkan ketidaklihatan skema ini. Prestasi skema yang dicadangkan dinilai secara eksperimen untuk menentukan ketidaklihatan, keselamatan, keteguhan dan keupayaan. Imej piawai USC-SIPI digunakan sebagai set data penanda aras untuk penilaian prestasi dan perbandingan skema yang dicadangkan dibandingkan dengan kerja-kerja terdahulu. Rintangan skim yang dicadangkan diuji dengan statistik, χ^2, histogram dan serangan pengesanan analisis stega tak berstruktur. Nilai PSNR yang diperoleh menunjukkan pencapaian ketidaklihatan dan keselamatan yang lebih tinggi oleh Skema DGV yang dicadangkan di samping mengekalkan keupayaan yang lebih tinggi berbanding kerja-kerja terdahulu. Ringkasnya, skema steganografi yang dicadangkan ini mengatasi prestasi skim penyembunyian data yang sedia ada secara komersial, sehingga dapat menyelesaikan masalah yang sedia ada.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DCT	-	Discrete Cosine Transform
χ^2	-	Chi-square
DE	-	Difference Expansion
DE	-	Difference Expansion
DFT	-	Discrete Fourier Transform
DGV	-	Distinction Grade Value
EC	-	Embedding Capacity
ER	-	Error Rate
FFT	-	Fractional Fourier Transform
FL	-	Fuzzy Logic
GA	-	Genetic Algorithm
HDWT	-	Haar Discrete Wavelet Transform
HVS	-	Human Visual System
ISS	-	Image Steganography Scheme
JPEG	-	Joint Photographic Experts Group
LSB	-	Least Significant Bit
MSB	-	Most Significant Bit
MSE	-	Mean Square Error
NCC	-	Normalized Cross-Correlation
PND	-	Random
PoV	-	Pairs of Values
PSNR	-	Peak Signal-to-Noise Ratio
PVD	-	Pixel Value Differencing
RGB	-	Red, Green and Blue
SIS	-	Steganography Image System
SSIM	-	Structural Similarity Index Measure
SSSM	-	Shuffle the Segments of Secret Message
SVM	-	Support Vector Machine
TCP/IP	-	Transmission Control Protocol/Internet Protocol
TIFF	-	Tagged Image File Format

WFFT	-	Weight Fractional Fourier Transform

LIST OF ALGORITHMS

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

In the internet era, sending and receiving data and information in the form of video, audio, image, and text become very easy. However, such easy access to the vast amount of information has posed severe threats to the security and privacy of the data. As such, securing the information over the non-secured public network is challenging. Often, the unauthorized users, intruders, attackers or adversaries can corrupt the information by manipulating the message, causing financial or ethical damages. Thus, to attain the secured data communications various information encryption and hiding schemes have been developed.

Over the last decade, many research efforts have been dedicated to develop Image Steganography Systems (ISSs). These systems gained the popularity due to the easy communication of the multimedia content through low-cost devices like mobiles and IP cameras, and social media like WhatsApp, Twitter, and Facebook. (Hussain *et al.*, 2018). In addition to the understanding of the secret data embedding in an image, several issues involving the image security and hiding of the secret message still remain unsolved (Sahu and Swain, 2020). Several studies revealed the substantial applications of the steganography in the field of medical diagnoses (Arunkumar *et al.*, 2019; Eze *et al.*, 2019), military (Tuncer and Avci, 2016), multimedia biometric data security (Mohsin *et al.*, 2018) and cloud computing (Shanthakumari and Malliga, 2019). The remaining key issues and difficulties related to the steganography are mainly divided into three types, i.e. (1) the inability to embed higher amount of data due to the limited payload capacity, (2) low security of the secret message hidden in the image, and (3) inability to maintain a high level of robustness and imperceptibility of the steganography system. Figure 1.1 shows these issues. Despite intensive research efforts these problems are far from being resolved. Thus, the current study made an effort to overcome these shortcomings.

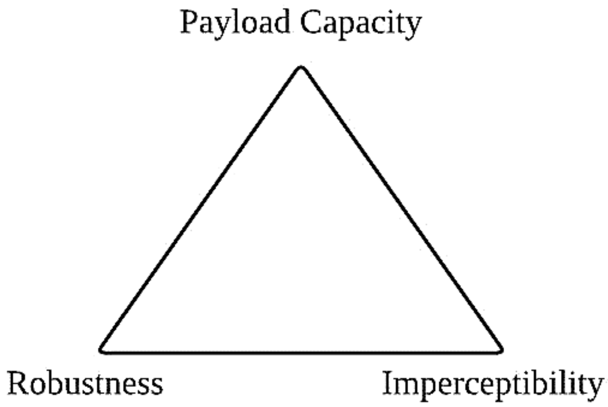

Figure 1.1 Key issues related to the existing steganography systems.

The steganography can be categorized into several types depending on the cover medium including the image, audio, text, video, DNA or even protocol (Hussain *et al.*, 2018). Each of these cover media has its advantage and drawbacks (Dhar and Banerjee, 2019; Kadhim *et al.*, 2019). Among these media, images are mostly used as a cover media due to their availability, easy usage by the users, high capacity and imperceptibility (Kadhim *et al.*, 2019; Subhedar and Mankar, 2020). As such, this study uses images as the cover media to host the text as a secret message.

As pointed out previously, the steganography is a method of hiding the sensitive data inside a trusted media such as an image so that it becomes unnoticeable by the intruders or unauthorized users. An image that hosts the secret data with a certain quality is called stego image, while the original image is called the cover image (Pak *et al.*, 2020). The importance of the stego is determined by the security of the secret message embedded inside the cover image. Another definition of the steganography is the data transfer over the Internet through the reliable media without noticing or discovering by the human eyes. There are two aspects of this description, the sender needs to hide the message and the receiver needs to extract the hidden message from the stego image via the information stored in the stego key (Gutub and Al-Ghamdi, 2020). Therefore, the main aim of the steganography is to maintain the stego image and then receive it without being noticed by the intruders or attackers

(Nisha and Monoth, 2020). The schematic diagram in Figure 1.2 depicts the working principle of a typical steganography model.

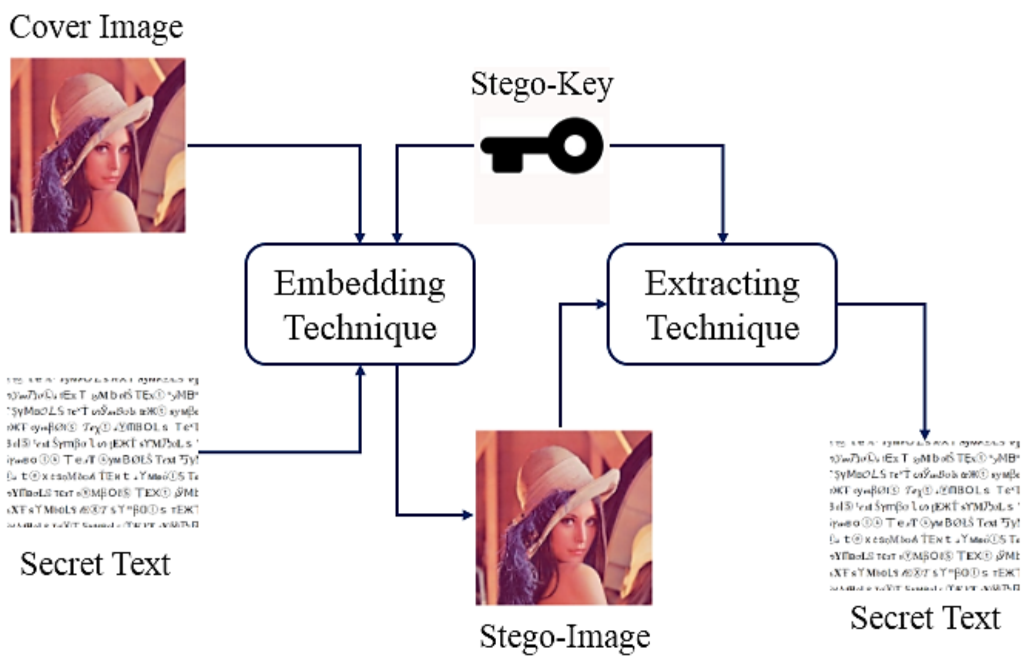

Figure 1.2 A block diagram of steganography model

The robustness of a steganography model depends on the suitability of the embedding process of the secret message in the cover image (Liao *et al.*, 2020). Furthermore, the stego key must include all the necessary information for extracting the secret message from the received image. The presence of any fault in certain steganography stage makes the scheme less secured (Gong *et al.*, 2020). A successful steganography system must support high capacity to carry more information, enhancing the security to make the system highly secured and reliability to ensure the imperceptibility of the system (Mukherjee and Jana, 2019). Furthermore, the imperceptibility determines the robustness of the steganography system (Edward Jero *et al.*, 2016). It is important to note that hackers are aware of the most of the existing steganography methods (Kadhim *et al.*, 2019). Thus, it is obligatory to devise a new steganography scheme with cutting-edge ideas so that they become less susceptible to the attacks. To this end, this thesis focuses on an improved embedding process for both secret message and cover image, which increases the capacity, imperceptibility and robustness of the proposed steganography scheme.

The basis of any steganography system is the embedding process to hide the secret data in the cover image which is achieved in three domains, namely spatial, transform and adaptive. The adaptive can essentially be interlinked to the spatial and transform domains (Hussain *et al.*, 2018; Kadhim *et al.*, 2019). Figure 1.3 shows the general classification domains of these domains used in the steganography systems. The simplest data embedding process for the digital images is based on the modification of the cover image pixels in the spatial domain (Nisha and Monoth, 2020). To encode the secret bit directly or indirectly, all these domains exploit the intensity of the pixels' level values of a cover image (Georges and Magdi, 2020). This is achieved via some mechanisms related to the embedding and decoding complexity. The spatial or image domain techniques use bit-wise methods that apply bit insertion and noise manipulation through modest mechanisms (Sidqi and Al-Ani, 2019). The Least Significant Bit (LSB) is the main spatial domain steganography scheme (Shanthakumari and Malliga, 2020). Most of the previous studies utilized the LSB method for embedding the secret bit into the image pixels to achieve high reliability and flexibility in the steganography system (Singh and Bhardwaj, 2019). Another reason for using the LSB method is its simplicity, high data embedding capacity and unrecognizable by the naked eyes (Hussain *et al.*, 2018).

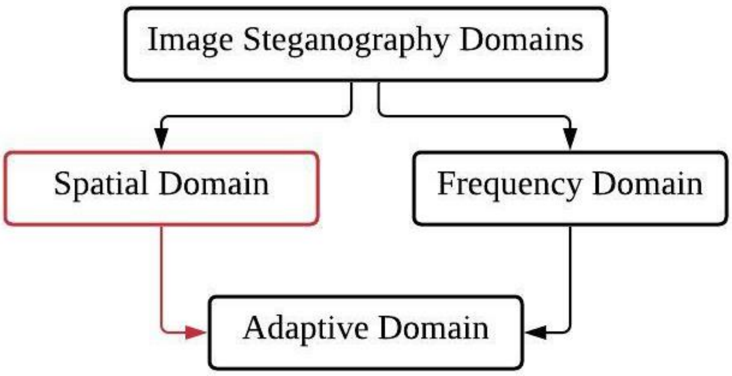

Figure 1.3 The general classification methods of different embedding domains

In the transform domain, on the other hand, the secret bits are embedded into the cover image wherein these bits are hidden under the sub-band frequency coefficients (Saidi *et al.*, 2019). Compared to the spatial domain, the process of embedment and extraction in the transform domain is very complex. Nevertheless, this approach does not only enhance the system security but also is less susceptible to cropping, compression, rotation and scaling attacks (Kadhim *et al.*, 2019). Therefore, the transform-based systems are more efficient in preserving the stego image quality, making less detectable in an unsecured channel. Several transform domain-based methods have been proposed for the steganography in which the most popular schemes include the Discrete Cosine Transform (DCT) (Saidi *et al.*, 2019) and Discrete Wavelet Transform (DWT) (Sharma *et al.*, 2019). Although the frequency domain-based steganography techniques have better security, they suffer the low imperceptibility and capacity(Kaur and Singh, 2020).

The adaptive domain combines both the spatial and transform domain (Yu *et al.*, 2020). In the data embedding process, the adaptive nature of the scheme can be included in various ways such as the selection of the target pixels in the cover image, number of bits embedded in a pixel and kind of modification to be made. However, the improved steganography schemes achieved involving the adaptive domain-based techniques need extra time-consuming procedures in advance including the compression, noise removal or encryption. In addition, these techniques are not effective for the embedding or hiding processes (Singh and Bhardwaj, 2019). Some ever-demanding applications of the steganography schemes related to the biometric screening and medical diagnoses need further recovery and improvement (Meng *et al.*, 2019). As pointed out previously, these applications still suffer low security and imperceptibility. As most of steganography schemes are real time programs, it is necessary that they are time efficient (Douglas *et al.*, 2018).

1.2 Problem Background

Hiding a message in the media such as images has received focused attention in the field of data security in the internet where attacks are very common. Lately, the internet providers have been paying more attention and playing significant role towards the information communication and transmission of various sensitive as well as private data. In this rationale, the data security became inevitable for the privacy preserved information transfer over the Internet. Earlier, many efforts have been dedicated to build secured steganography methods. However, the sensitive data to be concealed in media is not effective (Gutub and Al-Shaarani, 2020).In short, an accurate and robust steganography method with strong embedding process, security, and capacity is far from being achieved (Kadhim *et al.*, 2020).

Figure 1.4 shows fundamental features of an ISSs and the associated problems that need to be addressed. The challenges of the existing image steganography methods and limitations concerning the embedding solutions are emphasized. The highlighted requirements must be fulfilled during the design of the image steganography scheme. An ISSs with excellent security, high payload capacity and accurate embedding process have been deficient. In addition, the security of the secret message and payload capacity of the hidden data inside the stego image need to be enhanced. The embedding method must be able to improve the imperceptibility, wherein a new random partitioning technique can be used to enhance the robustness of the proposed scheme. The following sections discuss the main requirements and problems related to the existing ISSs that are addressed in this study.

Image Steganography Systems ISSs

1- Exposure to different kinds of attacks like HVS, Histogram and Chi-square (X^2) that makes the hidden secret message vulnerable to the attacks.
2- Ease of embedded secret data retrieval due to the use of weak encryption algorithms.
3- Have limited payload capacity in terms of the amount of data embedded to the image.
4- The low imperceptibility of the steganography method affects the system quality.

⇩

What Do We Need?

Need a solution that guarantees the high imperceptibility of the stego image while maintaining the payload capacity and security of the scheme as high as possible.

⇩

Limitations of the Existing ISSs Works

1- Use a portion of the image pixels such as a high contrast pixel value, edge region, and ROI only led to low capacity ('An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection', 2018) . .
2- Use known encryption methods effect negatively on the ISSs. on two ways. First, some known encryption methods have been breached by hackers, this, in turn, affects the robustness of the secret text as it is easy to retrieve. Second, the current encryption methods require a very long encryption key for which in turn requires reserving large areas of the vector that is responsible to hold the encryption information to the recipient's side inside the stego image which in turn reduce the imperceptibility of the stego imaeg3-High MSE that reduces the PSNR (Zodpe and Sapkal, 2020).
3- The use of image pixels in a binary manner has become known to intruders, which makes it easier to retrieve the embedded data (Kumar and Singh, 2020).
4- Use random methods to select blocks and pixels of the cover image with a one random parameter technique reduces the robustness (Mukherjee et al., 2020).

⇩

The Required Solution Must Achieve

1- A high level of security for the secret message via the synergy of the new encryption method and enhanced compression coding.
2- A high payload capacity via the use of enhanced compression coding and extend the pixel's value using the non-binary method.
3- Scheme with an integrated level of security by combining a new embedding method, divided the image into blocks and pixels randomly, a scanning algorithm between pixels that are under the threshold with the new coding method.
4- A high level of Robustness through the use of image decomposition and a random partitioning technique.

Figure 1.4 The problems that need to be addressed and resolved in the existing ISSs

The sensitive data (for example financial, banking, military, critical intelligence and medical) sent through the Internet needs absolute protection from the hackers and intruders interventions (Sedighi *et al.*, 2016; Pandey *et al.*, 2019). Due to the widespread nature of the images used in numerous applications over the internet, the images have been selected as the appropriate media to hold the transferred data. In addition, the data security becomes more important and challenging during the embedding to the image before sending it through any channels. Although several steganography methods have been proposed to address these challenges (Alyousuf *et al.*, 2020). However, the attackers have the ability to overcome those measures and easily introspect the hidden data embedded within the stego images (Jin *et al.*, 2020). Therefore, it is imperative to protect the stego image from being analyzed by the attackers. (Mahana and Aggarwal, 2019).

The security performance of any steganography method is determined by the amount of data hidden in the stego image. To maintain highly secured stego image , existing works tend to reduce the data embedded into it (Kadhim *et al.*, 2020). The intuition is that, the steganography developers try to keep the stego image as original as possible (Arunkumar *et al.*, 2019; Prasad and Pal, 2019). However, such approach adversely affects the capacity of the stego image, and consequently, limits the ability of the steganography system to only embed small amount of data into the cover image. As such, any proposed solution needs to increase the imperceptibility while maintaining high capacity.

Existing secret message encryption techniques used in steganograpy added an extra layer of security to make the steganography method secured (Zodpe and Sapkal, 2020). Such encryption makes it difficult for the attackers to reveal the content of the secret message even if the steganography method was compromised by steganalysis techniques. Although, many encryption methods have been suggested in the literature to improve the security of the payload, these methods are susceptible to cryptanalysis attacks. This is because these techniques rely on the changes in the order of bits, letters, or words which in turn depends on the random number generators to generate the encryption key (Stojanovski and Kocarev, 2001; Abdullatif *et al.*, 2018). Fundamentally, the random number generators are used to produce the encryption key used to encrypt the secret text. Usually, two types of random number generators are utilized including the True Random Number Generator (TRNG) and Pseudo-Random Number Generator (PRNG). The TRGN relies on entropy as a non-deterministic approach to implement the randomness. This gives the TRGN the ability to generate a difficult-to-break encrypted text. However, the TRNG is a time-consuming technique, which makes non-practical when dealing with large size of the text (Fadhel *et al.*, 2017). This means the TRNG technique requires a long encryption key, which in turn occupies more space from the vector which is responsible for carrying the encryption information in the stego image. Additionally, TRNG can be statistically analyzed, which facilitates decoding the cypher text.

In an image steganography system, the "security" is the vital characteristic that needs proper performance evaluation. The key requirement of the steganography system is to transmit the data securely so that the data remain inaccessible by the intruders during transmission through unsecured channels ('An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection', 2018) . The security refers to the "un-detectability" or "un-noticeability" of the steganography system (Prasad *et al.*, 2020). Thus, any steganography method is considered to be secured if the secret data remains undetectable by the statistical analysis or removal after being detected by the attacker. Generally, the steganography methods may suffer from various types of steganalysis detection attacks wherein the intruders try to detect the existence or even to retrieve the secret data embedded in the stego image (Karampidis *et al.*, 2018). To address this issue, a steganography system based on the Pixel Value Difference, text encryption and random pixel section was proposed to protect the stego message during transmission (Mukherjee *et al.*, 2020). Similarly, a bit-plane histogram-shifting based embedding was proposed by Nyeem (2018) . However, these methods can be statistically analyzed, which facilitates decoding the secret text (Hussain *et al.*, 2018; Kadhim *et al.*, 2019). Consequently, existing steganography systems still suffer from several types of attacks and needs further enhancement (Bachrach and Shih, 2017).

The primary aim of an efficient image steganography system is to send the maximum amount of data using the minimum pixels of the cover media. It enables reducing the interception probability while sending through an insecure channel and thereby demands high embedding capacity. According to Nyeem (2018) the embedding rate is the amount of hidden data (in bits) compared to the original image size. Keeping higher payload capacity without sacrificing the imperceptibility and security is a major challenge in the steganography system development (Kadhim *et al.*, 2019).

One of the prerequisites of any message embedding process is the imperceptibility which hides the secret bits in the digital image so that it remains invisible to the naked eye or statistics (Rawat *et al.*, 2020). The embedding process is inherently related to the payload volume of the secret data and security of the steganography system. Therefore, any reduction in the embedded data to the cover image can make little alteration of the bits in the original image. This keeps the stego image almost similar to the original image (Kuo *et al.*, 2016; Gutub and Al-Shaarani, 2020). The image quality of a steganography method is evaluated using the peak signal to noise ratio (PSNR) measure (Mahana and Aggarwal, 2019). The PSNR value is calculated by comparing the original and stego images after performing the embedding process. The data embedding process is considered to be imperceptible to the human vision system (HVS) if the PSNR value is greater than or equal to 30 dB (Al-tamimi and Alqobaty, 2015).

Over the past decades, the developers of the image steganography and steganalysis have paid much attention to enhance the PSNR value during the evaluation of the image steganography system (Vikranth *et al.*, 2015; Gutub and Al-Shaarani, 2020). Although different proposed techniques improved the PSNR, they could not maintain an acceptable level of the payload capacity (Seyyedi *et al.*, 2016; Saidi *et al.*, 2017). Thus, an accurate embedding method is still required to maintain the trade-off between security and imperceptibility of the stage image and increase the robustness of the steganography system. Few studies have been tried to reduce the value of the mean square error (MSE) for the embedding process to enhance the PSNR values (ALabaichi *et al.*, 2020). However, this comes at the cost of imperceptibility of the stego image, and consequently the robustness of the steganography system. As such, there is a need to address this issue and by building a robust steganography method that guarantees the security, capacity, imperceptibility of the stego image.

1.3 Problem Statement

There are several issues in the existing image steganography systems that need to be overcome. Firstly, payload security must be improved to prevent attackers from read the contents of hidden message even if they managed to analyse the stego image. These methods are well-known to intruders, which make it to reveal the secret text once detected in the stego image. Addition, the conventional encryption algorithms generate a long encryption key, which large space in the stego image. Consequently, it becomes easy for intruders to identify notice the hidden data in the stego image. Secondly, existing solutions suffer from high rate of MSE which decreases imperceptibility of the stego image and adversely affects the robustness of the steganography system(Kini and Kini, 2019). Thus, it is important that the steganography solutions address this issue and decrease MSE to improve the imperceptibility of the stego image.

In addition, existing steganography solutions suffer low embedding capacity. Although some of these solutions employed several compression techniques to compress the secret message before embedding, their concern was to reduce the size of the secret text. Such a reduction is suboptimal as it overlooks the capacity limitation of the stego image. For an effective steganography system, it is important to decrease the size of secret text while increasing the capacity of the stego image. Thus, a new scheme is needed for expanding the decomposition of the pixel value to enhance the capacity.

1.4 Research Aims

The aim of this study is to propose an improved image steganography scheme by increasing the security of the payload and capacity of the stego image while maintaining high imperceptibility.

1.5 Research Objectives

1. To improve the proposed scheme by integrating a new encryption method and enhanced compression algorithm for the secret message which increases the capacity while maintaining a higher level of security.
2. To enhance the robustness of the proposed steganography scheme by design a decomposition method while maintaining the visual quality of the stego image.
3. To propose and design a new embedding method for hiding the secret message which improves the security of the steganography scheme.

1.6 Scope of the Study

This work intends to develop a highly secured image steganography system based on a new embedding method with image partitioning to achieve the strong imperceptibility, high PSNR and improved robustness. Some of the existing state-of-the-art techniques are used in the proposed system to further enhance its robustness. Based on these set objectives, the following scopes of study are emerged:

i. The manipulation of the image such as the zooming, rotation, scaling, etc. is not considered in this study in addition to the time.

ii. The embedment of the text file into an image was performed by considering the condition of the steganography system.

iii. The use of the colour and grey images (Tiffany, Cameraman, Lena, Baboon, Zelda, Couple and Peppers with pixels size of 512×512) from the standard dataset (SIPI) for the evaluation of the proposed scheme.

iv. Testing the robustness of the proposed scheme against Chi-Square attack, Histogram and HVS attack.

v. This study does not include the speed of the encryption process and its comparison with other studies

vi. The performance evaluation of the proposed image steganography system using the PSNR, MSE, NCC and SSIM.

1.7 Significance of the Study

The proposed scheme overcomes the limitations associated with the security, capacity and imperceptibility of the existing steganography systems. The newly developed scheme became more reliable in terms of both security and capacity. The security of the steganography scheme was enhanced while keeping the PSNR score very high. This study faced some problem regarding the capacity and lowering its dependency. The limitations suffered by the existing method in the embedding process (Karampidis *et al.*, 2018; Alyousuf *et al.*, 2020), were overcome using the proposed scheme. The performance evaluation results of the present steganography scheme showed improved capacity and security.

The designed steganography scheme may contribute to several applied fields of data communication such as the military, medical, cloud computing, and industry where high security and robustness is the priority. In the medical field, vital information is hidden in the medical data itself and sequence of DNA and propagated. This will help to avoid the leakage of private details in unauthorized hands. While in multimedia applications, steganography is often applied to mark the copy right information. This is termed as watermarking and here, the cover media have more significance than the secret data. In industry and corporate communication, authenticity and security are much important since unsafe communication may result in serious data leakage. Some applications are presented in the prosed study such as Smartsteg on mobile devices (Bucerzan *et al.*, 2013), securing multimodal biometric data (Mohsin *et al.*, 2018), protection of IP (Intellectual Properties) and embedding individual information in smart identity card are also available (Sengupta and Rathor, 2019). One of the advanced steganography techniques is to use it with an advanced data structure; it helps in securing a large amount of information. The end-to-end data transmission could be done with the actual file securely using meta information with it. With the use of advanced data structure, the problem of allocation in the hard-disk memory can be targeted and yield in addressing the big data problems (Mcmillan, 2014).

1.8 Thesis Outline

The thesis is comprised of 6 chapters and the organization as follows. Chapter 2 presents a critical review of the relevant literature on image steganography. A comprehensive classification based on the cover types, key types, embedding and extracting techniques, some weaknesses with sued. Chapter 3 describes the methodology of the research with a detailed framework and analyze the proposed image steganography scheme (data pre-processing, embedding and extracting processes) are explained in Chapter 4. The performance evaluation outcome of the developed image steganography scheme against different attacks and achieved results are highlighted in Chapter 5. Chapter 6 concludes the thesis with novelty, contribution and recommendations for future work.

REFERENCES

AbdelQader, Akram, and Fadel AlTamimi. 2017. A novel image steganography approach using multi-layers dct features based on support vector machine classifier. *The International Journal of Multimedia & Its Applications. https://doi. org/10.5121/ijma*.

Abdullatif, Firas A, Alaa A Abdullatif, and Amna al-Saffar. 2018. Hiding techniques for dynamic encryption text based on corner point. In *Journal of Physics: Conference Series*, IOP Publishing, 12027.

Abo Mousa, Sheren Mohammed. 2017. LSBs Steganography based on R-indicator. *LSBs Steganography Based on R-Indicator*.

Agarwal, Parth, Dhruve Moudgil, and S Priya. 2020. Encrypted transfer of confidential information using steganography and identity verification using face data. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, 155–66.

Ahmed, Rami K, and Imad J Mohammed. 2017. Developing a new hybrid cipher algorithm using DNA and RC4. *International Journal of Advanced Computer Science and Applications* 8(10): 171–76.

Akhtar, Nadeem. 2016. An efficient lossless modulus function based data hiding method. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Springer, 281–87.

Al-Harbi, Omnia Abdullah, Walaa Essa Alahmadi, and Asia Othman Aljahdali. 2020. Security analysis of DNA based steganography techniques. *SN Applied Sciences* 2(2): 1–10.

Al-Husainy, Mohammed Abbas Fadhil, and Diaa Mohammed Uliyan. 2019. A secret-key image steganography technique using random chain codes. *International Journal of Technology* 10(4): 731–40.

Al-Nofaie, Safia, Adnan Gutub, and Manal Al-Ghamdi. 2019. Enhancing arabic text steganography for personal usage utilizing pseudo-spaces. *Journal of King Saud University-Computer and Information Sciences*.

Al-tamimi, Abdul-gabbar Tarish, and Abdulmalek Abduljabbar Alqobaty. 2015. Image steganography using least significant bits (LSBs): A novel algorithm. *International Journal of Computer Science and Information Security; Pittsburgh* 13(1): 5500.

ALabaichi, Ashwak, Maisa'a Abid Ali Al-Dabbas, and Adnan Salih. 2020. Image steganography using least significant bit and secret map techniques. *International Journal of Electrical & Computer Engineering (2088-8708)* 10.

Alam, Shahzad, Tanvir Ahmad, and Mohammad Najmud Doja. 2017. A novel edge based chaotic steganography method using neural network. In *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, Springer, 467–75.

Alvi, Aleem Khalid, and Robin Dawes. 2013. Image steganography using fuzzy domain transformation and pixel classification. *Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE* 2013-Janua(January): 277–82.

Alyousuf, Farah Qasim Ahmed, Roshidi Din, and Alaa Jabbar Qasim. 2020. Analysis review on spatial and transform domain technique in digital steganography. *Bulletin of Electrical Engineering and Informatics* 9(2): 573–81.

Aroukatos, Nikolaos G, Kostas Manes, and Stelios Zimeras. 2016. Social networks medical image steganography using sub-fibonacci sequences. In *MHealth Ecosystems and Social Networks in Healthcare*, Springer, 171–85.

Arunkumar, S. et al. 2019. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement: Journal of the International Measurement Confederation* 139: 426–37.

Ashraf, Zubair, Mukul Lata Roy, Pranab K Muhuri, and Q M Danish Lohani. 2020. Interval Type-2 fuzzy logic system based similarity evaluation for image steganography. *Heliyon* 6(5): e03771.

Bachrach, Mayra, and Frank Y. Shih. 2017. Survey of image steganography and steganalysis. *Multimedia Security: Watermarking, Steganography, and Forensics*: 201–14.

Bao, Zhenkun et al. 2019. A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. *Journal of Ambient Intelligence and Humanized Computing* 11(5): 1889–1901.

Bedi, Punam, and Arti Dua. 2020. Network steganography using the overflow field of timestamp option in an IPv4 packet. *Procedia Computer Science* 171: 1810–18.

Bennett, Krista. 2004. West Lafayette, Indiana, USA: Centre for Education, research om onformation assurance, and security, Purdue University *Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text*.

Bharti, Shambhu Shankar, Manish Gupta, and Suneeta Agarwal. 2019. A novel approach for audio steganography by processing of amplitudes and signs of secret audio separately. *Multimedia Tools and Applications* 78(16): 23179–201.

Bhattacharyya, Souvik, Aparajita Khan, and Gautam Sanyal. 2014. DCT difference modulation (DCTDM) image steganography. *International Journal of Information and Network Security* 3(1): 40.

Bheda, Eshita et al. 2013. Multimedia steganography with cipher text and compression. *International Journal of Emerging Technology and Advanced Engineering* 3(4): 322–24.

Bilal, Muhammad, Sana Imtiaz, Wadood Abdul, and Sanaa Ghouzali. 2013. Zero-steganography using DCT and spatial domain. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*.

Birajdar, Gajanan K, Vishwesh A Vyawahare, and Mukesh D Patil. 2018. Secure and robust ECG steganography using fractional fourier transform. *Cryptographic and Information Security Approaches for Images and Videos*: 19.

Biswas, Rajib, and Samir Kumar Bandyapadhay. 2019. Random selection based GA optimization in 2D-DCT domain color image steganography. *Multimedia Tools and Applications*: 1–20.

Böhme, Rainer. 2010. Principles of modern steganography and steganalysis. *Information Security and Cryptography* (9783642143120): 11–77.

Bower, Amanda et al. 2015a. The distribution of gaps between summands in generalized Zeckendorf decompositions. *Journal of Combinatorial Theory. Series A* 135: 130–60. http://dx.doi.org/10.1016/j.jcta.2015.04.005.

Bower, A., Insoft, R., Li, S., Miller, S. J., & Tosteson, P.. 2015b. The distribution of gaps between summands in generalized Zeckendorf decompositions. *Journal of Combinatorial Theory, Series A* 135: 130–60.

Bucerzan, Dominic, Crina Raţiu, and Misu Jan Manolescu. 2013. SmartSteg: A new android based steganography application. *International Journal of Computers, Communications and Control* 8(5): 681–88.

Cancelli, Giacomo, Gwenaël Doërr, Mauro Barni, and Ingemar J Cox. 2008. A comparative study of±steganalyzers. In *2008 IEEE 10th Workshop on Multimedia Signal Processing*, IEEE, 791–96.

Chakraborty, Soumendu, Anand Singh Jalal, and Charul Bhatnagar. 2017. LSB based non blind predictive edge adaptive image steganography. *Multimedia Tools and Applications* 76(6): 7973–87.

Chang, Chin Chen, Yi Hui Chen, and Chia Chen Lin. 2009. A Data Embedding scheme for color images based on genetic algorithm and absolute moment Block Truncation Coding. *Soft Computing* 13(4): 321–31.

Chang, Chin Chen, Yuan Hui Yu, and Yu Chen Hu. 2008. Hiding secret data into an AMBTC-compressed image using genetic algorithm. *Proceedings of the 2008 2nd International Conference on Future Generation Communication and Networking, FGCN 2008* 3: 154–57.

Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. 2010. Digital image steganography: survey and analysis of current methods. *Signal Processing* 90(3): 727–52. http://dx.doi.org/10.1016/j.sigpro.2009.08.010.

Chowdhuri, Partha, Biswapati Jana, and Debasis Giri. 2018. Secured steganographic scheme for highly compressed color image using weighted matrix through DCT. *International Journal of Computers and Applications* 7074.

Das, Madhulina, and Samir Kumar Bandyopadhyay. 2015. Survey and analysis of current methods of steganography. *International Journal of modern Trends in Engineering and Research* 2(7): 527–37.

Dhaked, Devender, Surendra Yadav, Manish Mathuria, and Saroj Agrawal. 2019. User identification over digital social network using fingerprint authentication. In *Emerging Trends in Expert Applications and Security*, Springer, 11–22.

Dhall, Sangeeta, Rinku Sharma, and Shailender Gupta. 2020. A multi-level steganography mechanism using quantum chaos encryption. *Multimedia Tools and Applications* 79(3): 1987–2012.

Dhar, Mili, and Subhasish Banerjee. 2019. An efficient and enhanced mechanism for message hiding based on image steganography Using ECC-cryptosystem. In *Advances in Communication, Devices and Networking*, Springer, 461–72.

Douglas, Mandy, Karen Bailey, Mark Leeney, and Kevin Curran. 2018. An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications* 77(13): 17333–73.

Dumitrescu, Dragoş, Ioan-Mihail Stan, and Emil Simion. 2017. Steganography techniques. *Cryptology ePrint Archive*: 1–20.

Edward Jero, S., Palaniappan Ramu, and Ramakrishnan Swaminathan. 2016. imperceptibility - robustness tradeoff studies for ECG steganography using continuous ant colony optimization. *Expert Systems with Applications* 49: 123–35.

Erdas, Mehmet Levent, and Abdullah Emre Caglar. 2018. Analysis of the relationships between bitcoin and exchange rate, commodities and global indexes by asymmetric causality test. *Eastern Journal of European Studies* 9(2): 27.

Eze, Peter, Udaya Parampalli, Robin Evans, and Dongxi Liu. 2019. Integrity verification in medical image retrieval systems using spread spectrum steganography. *ICMR 2019 - Proceedings of the 2019 ACM International Conference on Multimedia Retrieval*: 53–57.

Fadhel, Sabah, Mohd Shafry, and Omar Farook. 2017. Chaos image encryption methods: A survey study. *Bulletin of Electrical Engineering and Informatics* 6(1): 99–104.

Fadhil, Ammar Mohammedali. 2016. Bit inverting map method for improved steganography scheme.

Fakhredanesh, Mohammad, Mohammad Rahmati, and Reza Safabakhsh. 2019. Steganography in discrete wavelet transform based on human visual system and cover model. *Multimedia Tools and Applications* 78(13): 18475–502.

Farrag, Sara, and Wassim Alexan. 2019. Secure 2D image steganography using Recamán's sequence. *Proceedings - 2019 International Conference on Advanced Communication Technologies and Networking, CommNet 2019*: 1–6.

Gambhir, Ankit, and Rajeev Arya. 2019. Performance analysis and implementation of DES algorithm and RSA algorithm with image and audio steganography techniques. In *Computing, Communication and Signal Processing*, Springer, 1021–28.

Gaurav, Kumar, and Umesh Ghanekar. 2018. Image steganography based on canny edge detection, dilation operator and hybrid coding. *Journal of Information Security and Applications* 41: 41–51.

Georges, Jeanne, and Dalia A Magdi. 2020. Using artificial intelligence approaches for image steganography: A review. In *Internet of Things—Applications and Future*, Springer, 239–47.

Ghebleh, M., and A. Kanso. 2014. A robust chaotic algorithm for digital image steganography. *Communications in Nonlinear Science and Numerical Simulation* 19(6): 1898–1907.

Gong, Xinhui et al. 2020. A Secure Image Authentication Scheme Based on Dual Fragile Watermark. *Multimedia Tools and Applications*: 1–18.

Grajeda-Marín, Ismael R. et al. 2018. A new optimization strategy for solving the fall-off boundary value problem in pixel-value differencing steganography. *International Journal of Pattern Recognition and Artificial Intelligence* 32(1): 1–17.

Grajeda-Marín, Ismael R et al. 2016. An optimization approach to the TWPVD method for digital image steganography. In *Mexican Conference on Pattern Recognition*, Springer, 125–34.

Gurunathan, K, and S P Rajagopalan. 2020. A stegano-visual cryptography technique for multimedia security. *Multimedia Tools and Applications* 79(5): 3893–3911.

Gutub, Adnan, and Maimoona Al-Ghamdi. 2020. Hiding shares by multimedia image steganography for optimized counting-based secret sharing. *Multimedia Tools and Applications* 79(11–12): 7951–85.

Gutub, Adnan, and Faiza Al-Shaarani. 2020. efficient implementation of multi-image secret hiding based on LSB and DWT steganography Comparisons. *Arabian Journal for Science and Engineering*: 1–14.

Heidari, Shahrokh et al. 2019. A new general model for quantum image histogram (QIH). *Quantum Information Processing* 18(6): 1–20.

Huang, Chiung-Wei, Changmin Chou, Yu-Che Chiu, and Cheng-Yuan Chang. 2018. Embedded FPGA design for optimal pixel adjustment process of image steganography. *Mathematical Problems in Engineering* 2018: 1–8.

Huffman, David A. 1952. A method for the construction of minimum-redundancy codes. *Proceedings of the IRE* 40(9): 1098–1101.

Hussain, Mehdi et al. 2018. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication* 65(December 2017): 46–66.

Hussain, Mehdi, and Mureed Hussain. 2013. A survey of image steganography techniques. *International Journal of Advanced Science and Technology* 54: 113–24.

Islam, Mohiul, and Rabul Hussain Laskar. 2018. Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM. *Multimedia Tools and Applications* 77(11): 14407–34.

Islam, Mohiul, Amarjit Roy, and Rabul Hussain Laskar. 2018. Neural network Based robust image watermarking technique in LWT domain. *Journal of Intelligent & Fuzzy Systems* 34(3): 1691–1700.

Jain, Nitin, Sachin Meshram, and Shikha Dubey. 2012. Image steganography using LSB and edge–detection technique. *International Journal of Soft Computing and Engineering (IJSCE) ISSN* 223.

Jansi, K R, and Sakthi Harshita Muthusamy. 2020. Steganographic approach to enhance secure data communication using nonograms. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, 701–12.

Jiang, Nan et al. 2019. Quantum image encryption based on Henon mapping. *International Journal of Theoretical Physics* 58(3): 979–91.

Jin, Zhiyang, Guorui Feng, Yanli Ren, and Xinpeng Zhang. 2020. Feature extraction optimization of JPEG steganalysis based on residual images. *Signal Processing* 170: 107455.

Jude Hemanth, D., J. Anitha, Daniela Elena Popescu, and Le Hoang Son. 2018. A modified genetic algorithm for performance improvement of transform based image steganography systems. *Journal of Intelligent and Fuzzy Systems* 35(1): 197–209.

Kadhim, Inas Jawad, Prashan Premaratne, and Peter James Vial. 2020. High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. *Cognitive Systems Research* 60: 20–32.

Kadhim, Inas Jawad, Prashan Premaratne, Peter James Vial, and Brendan Halloran. 2019. Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing* 335: 299–326.

Karadogan, I, and R Das. 2014. An examination on information hiding tools for steganography. *International Journal of Information Security Science* 3(3): 200–208.

Karampidis, Konstantinos, Ergina Kavallieratou, and Giorgos Papadourakis. 2018. A review of image steganalysis techniques for digital forensics. *Journal of information security and applications* 40: 217–35.

Karem M, Mohammed A, and Ahmed Sami Nori. 2020. Blind steganalysis using one-class classification. *AL-Rafidain Journal of Computer Sciences and Mathematics* 13(2): 28–41.

Kasapbaşi, Mustafa Cem. 2019. A new chaotic image steganography technique based on Huffman compression of Turkish texts and fractal encryption with post-quantum security. *IEEE Access* 7: 148495–510.

Kaur, Mohanjeet, and Mamta Juneja. 2017. Adaptive block based steganographic model with dynamic block estimation with fuzzy rules. In *Innovations in Computer Science and Engineering*, Springer, 167–76.

Kaur, Rajwinder, and Butta Singh. 2020. A hybrid image steganography using chaotic maps in DCT domain. In *Soft Computing: Theories and Applications*, Springer, 649–59.

Kaur, Ravpreet, and Manish Mahajan. 2016. Random pattern based sequential bit (RaP-SeB) steganography with cryptography for video embedding. *International Journal of Modern Education and Computer Science* 8(9): 51–59.

Khan, Sahib, Nasir Ahmad, and Muneeza Wahid. 2016. Varying index varying bits substitution algorithm for the implementation of VLSB steganography. *Journal of the Chinese Institute of Engineers, Transactions of the Chinese Institute of Engineers,Series A* 39(1): 101–9.

Kiani, Soheila, and Mohsen Ebrahimi Moghaddam. 2009. Fractal based digital image watermarking using fuzzy C-mean clustering. *Proceedings - 2009 International Conference on Information Management and Engineering, ICIME 2009*: 638–42.

Kini, N Gopalakrishna, and Vishwas G Kini. 2019. A parallel algorithm to hide an image in an image for secured steganography. In *Integrated Intelligent Computing, Communication and Security*, Springer, 585–94.

Klein, Shmuel Tomi, Shoham Saadia, and Dana Shapira. 2019. Forward looking Huffman coding. In *International Computer Science Symposium in Russia*, Springer, 203–14.

Knapp, Jason F, and Steve W Worrell. 2015. Multi-scale image normalization and enhancement.

Kumar, Ravinder, and Hitesh Singh. 2020. Recent trends in text steganography with experimental study. In *Handbook of Computer Networks and Cyber Security*, Springer, 849–72.

Kumar, Vijay, and Dinesh Kumar. 2018. A modified DWT-based image steganography technique. *Multimedia Tools and Applications* 77(11): 13279–308.

Kuo, Wen Chung, Chun Cheng Wang, and Hong Ching Hou. 2016. Signed digit data hiding scheme. *Information Processing Letters* 116(2): 183–91.

Li, Mengdi et al. 2019. Generating steganographic image description by dynamic synonym substitution. *Signal Processing* 164: 193–201.

Liao, Xin et al. 2020. A new payload partition strategy in color image steganography. *IEEE Transactions on Circuits and Systems for Video Technology* 30(3): 685–96.

Lu, Wei, Ruipeng Li, et al. 2019. Binary image steganalysis based on histogram of structuring elements. *IEEE Transactions on Circuits and Systems for Video Technology*.

Lu, Wei, Liyu He, et al. 2019. Secure binary image steganography based on fused distortion measurement. *IEEE Transactions on Circuits and Systems for Video Technology* 29(6): 1608–18.

Mahajan, Manish, and Navdeep Kaur. 2012. Adaptive steganography: A survey of recent statistical aware steganography Techniques. *International Journal of Computer Network and Information Security* 4(10): 76.

Mahana, Sumit Kumar, and Rajesh Kumar Aggarwal. 2019. Image steganography: analysis & evaluation of secret communication. *SSRN Electronic Journal*: 1936–43.

Mahdi, Mohammed Hashim et al. 2019. Improvement of image steganography scheme based on LSB value with two control random parameters and multi-level encryption. *IOP Conference Series: Materials Science and Engineering* 518(5): 0–14.

Mandal, Jyotsna Kumar. 2020. Discrete fourier transform-based steganography. In *Reversible Steganography and Authentication via Transform Encoding*, Springer, 63–98.

Mandal, Kunal Kumar et al. 2020. Applying encryption algorithm on text steganography based on number system. In *Computational Advancement in Communication Circuits and Systems*, Springer, 255–66.

Maniriho, Pascal, and Tohari Ahmad. 2019. Information hiding scheme for digital images using difference expansion and modulus function. *Journal of King Saud University - Computer and Information Sciences* 31(3): 335–47.

Mante, Pratik Gajanan, Harsh Rajendra Oswal, Debabrata Swain, and Deepali Deshpande. 2020. A symmetrical encryption technique for text encryption using randomized matrix based key generation. In *Advances in Data Science and Management*, Springer, 137–48.

Maurya, Indu, and S K Gupta. 2019. Understandable Huffman coding: a case study. In *Soft Computing: Theories and Applications*, Springer, 147–58.

Meng, Ruohan et al. 2019. A novel steganography scheme combining coverless information hiding and steganography. *Journal of Information Hiding and Privacy Protection* 1(1): 43–48.

Mohsin, A. H. et al. 2018. Real-time medical systems based on human biometric steganography: A systematic review. *Journal of Medical Systems* 42(12).

Mondal, Bhaskar, Tarni Mandal, Punj Kumar, and Neel Biswas. 2018. A secure partial encryption scheme based on bit plane manipulation. *2017 7th International Symposium on Embedded Computing and System Design, ISED 2017* 2018-Janua: 1–5.

More, Shraddha, and Rajesh Bansode. 2015. Implementation of AES with time complexity measurement for various input. *Glob. J. Comput. Sci. Technol. E Netw. Web Secur* 15: 10–20.

Muhammad, Khan et al. 2016. A novel magic lsb substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimedia Tools and Applications* 75(22): 14867–93.

Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. 2017. CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications* 76(6): 8597–8626.

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. 2018. image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems* 86: 951–60.

Mukherjee, Nabanita, Goutam Paul, Sanjoy Kumar Saha, and Debanjan Burman. 2020. A PVD based high capacity steganography algorithm with embedding in non-sequential position. *Multimedia Tools and Applications*: 1–31.

Mukherjee, Subhadip, and Biswapati Jana. 2019. A novel method for high capacity reversible data hiding scheme using difference expansion. *International Journal of Natural Computing Research (IJNCR)* 8(4): 13–27.

Nayak, Rakesh. 2015. Steganography with BSS-RSA-LSB technique : A new approach to steganography . 3(5): 187–90.

Nguyen, Tuan Duc, Somjit Arch-Int, and Ngamnij Arch-Int. 2016. An adaptive multi Bit-Plane Image Steganography Using Block Data-Hiding. *Multimedia tools and applications* 75(14): 8319–45.

Nikam, Virendra P, and Shital S Dhande. 2019. Extended Fibonacci Series for selection of carrier samples in data hiding and extraction. In *International Conference on Intelligent Data Communication Technologies and Internet of Things*, Springer, 40–50.

Nisha, C D, and Thomas Monoth. 2020. Analysis of spatial domain image steganography based on pixel-value differencing method. In *Soft Computing for Problem Solving*, Springer, 385–97.

Nolkha, Avneesh, Sunil Kumar, and V S Dhaka. 2020. Image steganography using LSB substitution: A comparative analysis on different color models. In *Smart Systems and IoT: Innovations in Computing*, Springer, 711–18.

Nyeem, Hussain. 2018. Reversible data hiding with image bit-plane slicing. *20th International Conference of Computer and Information Technology, ICCIT 2017* 2018-Janua(December): 1–6.

Pak, Chanil et al. 2020. A novel color image LSB steganography using improved 1D chaotic map. *Multimedia Tools and Applications* 79(1–2): 1409–25.

Pal, Ratna. 2020. Further remarks on rigidity of Hénon maps. *Journal of Mathematical Analysis and Applications* 484(2): 123658.

Pandey, Anukul, Barjinder Singh Saini, Butta Singh, and Neetu Sood. 2019. Bernoulli's chaotic map-based 2D ECG image steganography: A medical data security approach. In *Medical Data Security for Bioengineers*, IGI Global, 208–41.

Patil, Rupali, and Dipak Pawar. 2016. Secure audio steganography by LSB for hiding information. *International Journal of Innovations in Engineering Research and Technology* 3(4): 1–6.

Petitcolas, Fabien. 1883. La Cryptographie Militaire.

Prasad, Prajith Kesava, R Kalpana Sonika, R Jenice Aroma, and A Balamurugan. 2020. Enhanced security credentials for image steganography using QR code. In *Smart Computing Paradigms: New Progresses and Challenges*, Springer, 259–66.

Prasad, Shiv, and Arup Kumar Pal. 2019. Logistic map-based image steganography scheme using combined LSB and PVD for security enhancement. In *Emerging Technologies in Data Mining and Information Security*, Springer, 203–14.

Prasetyadi, Gotfried C, Achmad Benny Mutiara, and Rina Refianti. 2017. File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method. In *2017 Second International Conference on Informatics and Computing (ICIC)*, IEEE, 1–5.

Qian, Zhenxing, Kim-Kwang Raymond Choo, Rémi Cogranne, and Xinpeng Zhang. 2018. Multimedia security: novel steganography and privacy preserving. *Security and Communication Networks* 2018.

Qu, Zhiguo et al. 2018. Anti-noise bidirectional quantum steganography protocol with large payload. *International Journal of Theoretical Physics* 57(6): 1903–27.

Raeiatibanadkooki, Mahsa, Saeed Rahati Quchani, Mohammad Mahdi KhalilZade, and Kambiz Bahaadinbeigy. 2016. Compression and encryption of ECG Signal using wavelet and chaotically Huffman code in telemedicine application. *Journal of Medical Systems* 40(3): 1–8.

Rahman, Mir Lutfur, Pranta Sarker, and Ahsan Habib. 2019. A faster decoding technique for Huffman codes using adjacent distance array. In *International Joint Conference on Computational Intelligence*, Springer, 309–16.

El Rahman, Sahar A. 2018. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. *Computers and Electrical Engineering* 70: 380–99.

Rai, Ankur, and Harsh Vikram Singh. 2017. SVM based robust watermarking for enhanced medical image security. *Multimedia Tools and Applications* 76(18): 18605–18.

Rai, A., & Singh, H. V.. 2018. Machine learning-based robust watermarking technique for medical image transmitted over LTE network. *Journal of Intelligent Systems* 27(1): 105–14.

Rajendran, Sujarani, and Manivannan Doraipandian. 2017. Chaotic Map Based Random Image Steganography Using LSB Technique. *International Journal of Network Security* 19(4): 593–98.

Ramalingam, Mritha, and Nor Ashidi Mat Isa. 2015. A Steganography Approach over Video Images To Improve Security. *Indian Journal of Science and Technology* 8(1): 79.

Rao, Ch Srinivasa, and V S Bharathi Devi. 2016. Comparative Analysis of HVS Based Robust Video Watermarking Scheme. In *Microelectronics, Electromagnetics and Telecommunications*, Springer, 103–10.

Rathor, Mahendra, and Anirban Sengupta. 2020. Design Flow Of Secured N-Point DFT Application Specific Processor Using Obfuscation And Steganography. *IEEE Letters of the Computer Society* 3(1): 13–16.

Rawat, Ritvik, Brijesh Singh, Arijit Sur, and Pinaki Mitra. 2020. Steganalysis for clustering modification directions steganography. *Multimedia Tools and Applications* 79(3–4): 1971–86.

Roy, Sangita, and Vivek Kapoor. 2020. High data rate audio steganography. In *International Conference on Innovative Computing and Communications*, Springer, 503–15.

Sabry, Mona, Taymoor Nazmy, and Mohamed Essam Khalifa. 2019. Steganography in DNA sequence on the level of amino acids. In *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, IEEE, 317–24.

Saeed, Ayesha et al. 2020. An accurate texture complexity estimation for quality-enhanced and secure image steganography. *IEEE Access* 8: 21613–30.

Sahu, Aditya Kumar, and Gandharba Swain. 2019. An optimal information hiding approach based on pixel value differencing and modulus function. *Wireless Personal Communications* 108(1): 159–74.

Sahu, Aditya Kumar, and Gandharba Swain. 2020. Reversible image steganography using dual-layer LSB matching. *Sensing and Imaging* 21(1). https://doi.org/10.1007/s11220-019-0262-y.

Saidi, Marwa et al. 2019. USAD: Undetectable Steganographic approach in DCT domain. *Imaging Science Journal* 67(5): 237–53.

Saidi, Marwa, Houcemeddine Hermassi, Rhouma Rhouma, and Safya Belghith. 2017. A new adaptive image steganography scheme based on DCT and chaotic map. *Multimedia Tools and Applications* 76(11): 13493–510.

Sailaja, C, and Srinivas Bachu. 2020. A comparative study on LSB replacement steganography. In *Innovations in Electronics and Communication Engineering*, Springer, 601–12.

Sairam, T D, and K Boopathybagan. 2019. Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods. *Automatika* 60(3): 285–93.

Sajasi, Sara, and Amir Masoud Eftekhari Moghadam. 2013. A high quality image steganography scheme based on fuzzy inference system. *13th Iranian Conference on Fuzzy Systems, IFSC 2013*.

Salem, Ali, Mohammed Sabbih, Hamoud Al-tamimi, and Alaa Ahmed. 2020. Secure image steganography through multilevel security. 11(1): 80–103.

Sari, Christy Atika, Giovani Ardiansyah, De Rosal Ignatius Moses Setiadi, and Eko Hari Rachmawanto. 2019. An improved security and message capacity using AES and Huffman coding on image steganography. *Telkomnika (Telecommunication Computing Electronics and Control)* 17(5): 2400–2409.

Sarmah, Dipti Kapoor, and Anand J. Kulkarni. 2018. JPEG Based Steganography methods using cohort intelligence with cognitive computing and modified multi random start local search optimization algorithms. *Information Sciences* 430–431: 378–96.

Sarmah, Dipti Kapoor, Anand J Kulkarni, and Ajith Abraham. 2020a. Cryptography and digital image steganography techniques. In *Optimization Models in Steganography Using Metaheuristics*, Springer, 33–48.

Sarmah, D. K., Kulkarni, A. J., & Abraham, A.. 2020b. Steganalysis on all approaches/vulnerability analysis of stego image (S). In *Optimization Models in Steganography Using Metaheuristics*, Springer, 147–61.

Satir, Esra, and Hakan Isik. 2014. A Huffman compression based text steganography method. *Multimedia tools and applications* 70(3): 2085–2110.

Savithri, G, Sayali Mane, and J Saira Banu. 2017. Parallel implementation of RSA 2D-DCT steganography and Chaotic 2D-DCT steganography. In *Proceedings of International Conference on Computer Vision and Image Processing*, Springer, 593–605.

Sedighi, Vahid, Rémi Cogranne, and Jessica Fridrich. 2016. Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security* 11(2): 221–34.

Sengupta, Anirban, and Mahendra Rathor. 2019. IP core steganography for protecting DSP kernels used in CE systems. *IEEE Transactions on Consumer Electronics* 65(4): 506–15.

Setiadi, De Rosal Ignatius Moses, and Jumanto Jumanto. 2018. An enhanced LSB-image steganography using the hybrid canny-sobel edge detection. *Cybernetics and Information Technologies* 18(2): 74–88.

Seyyedi, Seyyed Amin, Vasili Sadau, and Nick Ivanov. 2016. A Secure Steganography Method Based on Integer Lifting Wavelet Transform. *International Journal of Network Security* 18(1): 124–32.

Shankar, Deepa D, and Prabhat Kumar Upadhyay. 2020. Steganalysis of very low embedded JPEG image in spatial and transform domain steganographic scheme using SVM. In *Innovations in Computer Science and Engineering*, Springer, 405–12.

Shanthakumari, R., and S. Malliga. 2019. Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment. *Sadhana - Academy Proceedings in Engineering Sciences* 44(5): 1–12.

Shanthakumari, R., and S. Malliga.. 2020. Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. *Multimedia Tools and Applications* 79(5–6): 3975–91.

Sharma, Vijay Kumar, Pratistha Mathur, and Devesh Kumar Srivastava. 2019. Highly secure DWT steganography scheme for encrypted data hiding. In *Information and Communication Technology for Intelligent Systems*, Springer, 665–73.

Shen, Shuyuan, Lihong Huang, and Qinglong Tian. 2015. A novel data hiding for color images based on pixel value difference and modulus function. *Multimedia Tools and Applications* 74(3): 707–28.

Shyla, M K, and K B Shiva Kumar. 2019. Novel color image data hiding technique based on DCT and compressed sensing Algorithm. In *Emerging Research in Electronics, Computer Science and Technology*, Springer, 1151–57.

Sidqi, Haval Muhammed, and Muzhir Shaban Al-Ani. 2019. Image steganography: review study. In *Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV)*, The Steering Committee of The World Congress in Computer Science, Computer …, 134–40.

Simmons, Gustavus J. 1984. The prisoners' problem and the subliminal channel. *Advances in Cryptology, Sprigher-Verlag*: 51–67.

Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh. 2015. Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science* 54: 73–82.

Singh, Namrata, and Jayati Bhardwaj. 2019. Comparative analysis for steganographic LSB variants. In *Computing, Communication and Signal Processing*, Springer, 827–35.

Som, Sukalyan, Abhijit Mitra, Sarbani Palit, and B. B. Chaudhuri. 2019. A selective bitplane image encryption scheme using chaotic maps. *Multimedia Tools and Applications* 78(8): 10373–400.

Song, Xianhua, Shen Wang, and Xiamu Niu. 2012. An integer DCT and affine transformation based image steganography method. *Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2012*: 102–5.

Stojanovski, Toni, and Ljupco Kocarev. 2001. Chaos-based random number generators-Part I: Analysis [Cryptography]. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 48(3): 281–88.

Subhedar, Mansi S, and Vijay H Mankar. 2020. Secure image steganography using framelet transform and bidiagonal SVD. *Multimedia Tools and Applications* 79(3): 1865–86.

Sun, Shuliang. 2016. A novel edge based image steganography with 2k correction and Huffman encoding. *Information Processing Letters* 116(2): 93–99.

Swain, Gandharba. 2018a. Adaptive and non-adaptive PVD steganography using overlapped pixel blocks. *Arabian Journal for Science and Engineering* 43(12): 7549–62.

Swain, Gandharba. 2018b. High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis. *Security and Communication Networks* 2018.

Swain, Gandharba.. 2019. Very high capacity image steganography technique using quotient value differencing and LSB substitution. *Arabian Journal for Science and Engineering* 44(4): 2995–3004. https://doi.org/10.1007/s13369-018-3372-2.

Syahlan, Zainal, and Tohari Ahmad. 2019. Reversible data hiding method by extending reduced difference expansion. *International Journal of Advances in Intelligent Informatics* 5(2): 101–12.

Thampi, Sabu M. 2008. Information hiding techniques: A tutorial review. *CoRR*. http://arxiv.org/abs/0802.3746.

Thomas, Eric. 2015. The Fibonacci sequence through a different lens.

Thorat, Ashitosh S, and G. U. Kharat. 2015. Steganography based navigation of missile. *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)* 4(6): 1662–65.

Toosi, Ramin, Mohammadreza Sadeghi, and Mohammad Ali Akhaee. 2019. Robust image watermarking using sample area quantization. *Multimedia Tools and Applications* 78(24): 34963–80.

Tuncer, Türker, and Engin Avci. 2016. A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. *Displays* 41: 1–8.

Valandar, Milad Yousefi, Milad Jafari Barani, and Peyman Ayubi. 2020. A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map. *Soft Computing* 24(2): 771–94.

Vikranth, B M et al. 2015. A survey of image steganography. *Journal of Emerging Technologies and Innovative Research* 2(4).

Volkhonskiy, Denis, Ivan Nazarov, and Evgeny Burnaev. 2020. Steganographic generative adversarial networks. In *Twelfth International Conference on Machine Vision (ICMV 2019)*, International Society for Optics and Photonics, 114333M.

Wang, Jiaxin, Mengxin Cheng, Peng Wu, and Beijing Chen. 2019. A survey on digital image steganography.

Weber, Allan G. 1997. The USC-SIPI image database Version 5. *USC-SIPI Report* 315(1).

Yadav, Er R L, Er Chetan Kumar, and Er Raj Yadav. 2019. High capacity embedding and secured steganography model by using GA and integer wavelet Transform. (July).

Yang, Bohan, Vladimir Rozic, Nele Mentens, and Ingrid Verbauwhede. 2015. On-the-fly tests for non-ideal true random number generators. *Proceedings - IEEE International Symposium on Circuits and Systems* 2015-July: 2017–20.

Yeung, Yuileong et al. 2019. Secure binary image steganography based on LTP distortion minimization. *Multimedia Tools and Applications*.

Yi, Xiaowei et al. 2019. Ahcm: Adaptive Huffman code mapping for audio steganography based on psychoacoustic model. *IEEE Transactions on Information Forensics and Security* 14(8): 2217–31.

Younus, Zeyad Safaa, and Mohammed Khaire Hussain. 2019. Image steganography using exploiting modification direction for compressed encrypted data. *Journal of King Saud University - Computer and Information Sciences* (xxxx). https://doi.org/10.1016/j.jksuci.2019.04.008.

Yu, Xinzhi et al. 2020. Robust adaptive steganography based on generalized dither modulation and expanded embedding domain. *Signal Processing* 168: 107343.

Zodpe, Harshali, and Ashok Sapkal. 2020. An efficient AES implementation using FPGA with enhanced security features. *Journal of King Saud University-Engineering Sciences* 32(2): 115–22.

LIST OF PUBLICATIONS

Web of Science Journals

1. Hashim, M.M., Taha, M.S. , Rahim, M.S.M. “Concealing Critical Data in Medical Image by Emphasized Triple Decomposition for Worthiness: A novel Steganography Method”*, Multimedia Tools and Applications* (Q2) (Accepted).
2. Taha, Mustafa Sabah, et al. “High payload image steganography scheme with minimum distortion based on Distinction Grade Value method”, *Multimedia Tools and Applications* (Q2) (Submitted)

.

Scopus Journals

1. Taha, Mustafa Sabah, et al. "Information Hiding: A Tool for Securing Biometric Information." *Technology Reports of Kansai University / TRKU* , Vol. 62, Issue 04, April, 2020).
2. Mustafa, S. T., et al. "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*, Vol. 29, No. 7 s, (2020), pp. 2783-2801.
3. Hashim, M.M., Rahim, M.S.M., Johi, F.A., Taha, M.S. and Hamad, H.S., 2018. Performance evaluation measurement of image steganography techniques with analysis of lsb based on variation image formats. *International Journal of Engineering & Technology*, 7(4), pp.3505-3514.
4. Hashim, M.M., Rahim, M.S.M., Johi, F.A., Taha, M.S., Al-Wan, A.A. and Sjarif, N.N.A., 2018. An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching. *International Journal of Engineering & Technology*, 7(4), pp.4008-4023.
5. Qasim Mahdi Haref, Mustafa Sabah Taha*, Mohd Shafry Mohd Rahim, Mohammed Mahdi Hashim, 2018. Categorization of spatial domain techniques in image steganography: A revisit. *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 10, 13-Special Issue.
6. Maytham Mohammed Tuaama, Zainab Saad Karam, Mohammed Sabri Abuali, Mustafa Sabah Taha, Mohammed Mahdi Hashim, 2018. Review paper on

biometric data protection using Steganography techniques. Journal of Advanced Research in Dynamical and Control Systems, Vol. 10, 13-Special Issue.

Conference Paper

1. Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In *IOP conference series: materials science and engineering* (Vol. 518, No. 5, p. 052003). IOP Publishing.
2. Mahdi, M. H., Abdulrazzaq, A. A., Rahim, M. S. M., Taha, M. S., Khalid, H. N., & Lafta, S. A. (2019, May). Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. In *IOP Conference Series: Materials Science and Engineering* (Vol. 518, No. 5, p. 052002). IOP Publishing.
3. Hashim, M. M., Taha, M. S., Aman, A. H. M., Hashim, A. H. A., Rahim, M. S. M., & Islam, S. (2019, October). Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography. In *2019 7th International Conference on Mechatronics Engineering (ICOM)* (pp. 1-6). IEEE.
4. Naeem, M., Hameed, M., & Taha, M. S. (2020, February). A study of electronic payment system. In *IOP Conference Series: Materials Science and Engineering* (Vol. 767).
5. Abdulwahedand, M. N., Mustafa, S. T., & Rahim, M. S. M. (2019, October). Image Spatial Domain Steganography: A study of Performance Evaluation Parameters. In *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)* (pp. 309-314). IEEE.
6. Based on IoT Healthcare Application for Medical Data Authentication: Towards A new Secure Framework Using Steganography (Accepted)