# TRIPLE SCHEME BASED ON IMAGE STEGANOGRAPHY TO IMPROVE IMPERCEPTIBILITY AND SECURITY

MOHAMMED MAHDI HASHIM

UNIVERSITI TEKNOLOGI MALAYSIA

# TRIPLE SCHEME BASED ON IMAGE STEGANOGRAPHY TO IMPROVE IMPERCEPTIBILITY AND SECURITY

MOHAMMED MAHDI HASHIM

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

APRIL 2021

# 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 supervisor, Prof. Dr. Mohd Shafry Mohd Rahim for encouragement, guidance, critics, and friendship.

In preparing this thesis, I got engaged with many researchers, academics, and practitioners. Thus, I want to express my sincere appreciation to all my UTM academics professors' 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

A foremost priority in the information technology and communication era is achieving an effective and secure steganography scheme when considering information hiding. Commonly, the digital images are used as the cover for the steganography owing to their redundancy in the representation, making them hidden to the intruders. Nevertheless, any steganography system launched over the internet can be attacked upon recognizing the stego cover. Presently, the design and development of an effective image steganography system are facing several challenging issues including the low capacity, poor security, and imperceptibility. Towards overcoming the aforementioned issues, a new decomposition scheme was proposed for image steganography with a new approach known as a Triple Number Approach (TNA). In this study, three main stages were used to achieve objectives and overcome the issues of image steganography, beginning with image and text preparation, followed by embedding and culminating in extraction. Finally, the evaluation stage employed several evaluations in order to benchmark the results. Different contributions were presented with this study. The first contribution was a Triple Text Coding Method (TTCM), which was related to the preparation of secret messages prior to the embedding process. The second contribution was a Triple Embedding Method (TEM), which was related to the embedding process. The third contribution was related to security criteria which were based on a new partitioning of an image known as the Image Partitioning Method (IPM). The IPM proposed a random pixel selection, based on image partitioning into three phases with three iterations of the Hénon Map function. An enhanced Huffman coding algorithm was utilized to compress the secret message before TTCM process. A standard dataset from the Signal and Image Processing Institute (SIPI) containing color and grayscale images with 512 x 512 pixels were utilised in this study. Different parameters were used to test the performance of the proposed scheme based on security and imperceptibility (image quality). In image quality, four important measurements that were used are Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Square Error (MSE) and Histogram analysis. Whereas, two security measurements that were used are Human Visual System (HVS) and Chi-square ($X^2$) attacks. In terms of PSNR and SSIM, the Lena grayscale image obtained results were 78.09 and 1 dB, respectively. Meanwhile, the HVS and X2 attacks obtained high results when compared to the existing scheme in the literature. Based on the findings, the proposed scheme give evidence to increase capacity, imperceptibility, and security to overcome existing issues.

# ABSTRAK

Keutamaan terpenting dalam era teknologi maklumat dan komunikasi adalah mencapai skema steganografi yang berkesan dan selamat ketika mempertimbangkan penyembunyian maklumat. Biasanya, gambar digital digunakan sebagai penutup steganografi kerana kelebihannya dalam perwakilan, menjadikannya tersembunyi bagi penceroboh. Walaupun begitu, setiap sistem steganografi yang dilancarkan melalui internet dapat diserang setelah mengenali penutup stego. Pada masa ini, reka bentuk dan pembangunan sistem steganografi gambar yang berkesan menghadapi beberapa masalah yang mencabar termasuk kapasiti rendah, keselamatan yang lemah, dan tidak dapat dilihat. Untuk mengatasi masalah yang disebutkan di atas, skema penguraian baru diusulkan untuk steganografi gambar dengan pendekatan baru yang dikenali sebagai Pendekatan Nombor Tiga (TNA). Dalam kajian ini, tiga tahap utama digunakan untuk mencapai objektif dan mengatasi masalah steganografi gambar, dimulai dengan penyediaan gambar dan teks, diikuti dengan penyisipan dan memuncak dalam pengekstrakan. Akhirnya, peringkat penilaian menggunakan beberapa penilaian untuk membentuk penanda aras hasilnya. Sumbangan yang berbeza telah wujud dalam kajian ini. Sumbangan pertama adalah kaedah Pegkodan Teks Tiga Kali (TEM), yang berkaitan dengan proses embedding. Sumbangan ketiga berkaitan dengan kriteria keselamatan yang didasarkan pada pemisahan baru dari gambar yang dikenali sebagai Kaedah Pemisahan Imej (IPM). IPM mencadangkan pemilihan piksel secara rawak, berdasarkan pemisahan gambar menjadi tiga fasa dengan tiga lelaran fungsi Peta Hénon. Algoritma pengkodan Huffman yang diperkuat digunakan untuk memampatkan mesej rahsia sebelum proses TTCM. Set data standard dari Institut Pemprosesan Isyarat dan Imej (SIPI) yang mengandungi gambar warna dan skala kelabu dengan 512 x 512 piksel digunakan dalam kajian ini. Parameter yang berbeza digunakan untuk menguji prestasi skema yang dicadangkan berdasarkan keamanan dan ketidaklihatan (kualiti gambar). Dalam kualiti gambar, empat ukuran penting yang digunakan adalah Nisbah Puncak Isyarat-ke-Kebisingan (PSNR), Indeks Kesamaan Struktur (SSIM), Ralat Persegi Minimum (MSE) dan analisis Histogram. Manakala, dua ukuran keselamatan yang digunakan adalah serangan Sistem Visual Manusia (HVS) dan ki-kuadrat ($X^2$). Dari segi PSNR dan SSIM, gambar skala abu-abu Lena yang diperoleh masing-masing adalah 78.09 dan 1 dB. Sementara itu, serangan HVS dan X2 memperoleh hasil yang tinggi jika dibandingkan dengan skema yang ada dalam literatur. Berdasarkan penemuan tersebut, skema yang dicadangkan memberikan bukti untuk meningkatkan kapasiti, ketidaklihatan, dan keselamatan untuk mengatasi masalah yang ada.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| AES | - | Advanced Encryption Standard |
| ASCII | - | American Standard Code for Information Interchange |
| BIM | - | Bit Inversing Map |
| CBP | - | Complex Block Prior |
| CPB | - | Color Palette Based |
| DCT | - | Discrete Cosine Transform |
| DE | - | Difference Expansion |
| DES | - | Data Encryption Standard |
| DFT | - | Discrete Fourier Transform |
| DHR | - | Data Hiding Ratio |
| DNA | - | Deoxyribonucleic Acid |
| DWT | - | Discrete Wavelet Transform |
| ECC | - | Elliptic Curve Cryptography |
| EEG | - | Electroencephalogram |
| EMD | - | Exploiting Modification Direction |
| FRFT | - | Fractional Fourier Transform |
| GA | - | Genetic Algorithm |
| GLM | - | Gray Level Modification |
| HDWT | - | Haar Discrete Wavelet Transform |
| HPF | - | High Pass Filter |
| HVS | - | Human Visual Systems |
| IDFT | | Inverse Discrete Fourier Transform |
| IDWT | | Inverse Discrete Wavelet Transform |
| IP | - | Internet Protocol |
| ISSs | - | Image Steganography Systems |
| JPEG | - | Joint Photographic Experts Group |
| KT | - | Knight Tour |
| LSB | - | Least Significant Bit |
| LZW | - | Lempel Ziv Welch |
| MLE | - | Multi Level Encryption |

| | | |
|---|---|---|
| MR | - | Magnetic Resonance |
| MSB | - | Most Significant Bit |
| MSE | - | Mean Square Error |
| NCC | - | Normalized Correlation Coefficient |
| NUBASI | - | Non-Uniform Block of Adaptive Segmentation |
| OPAP | - | Optimal Pixels Adjustment Process |
| PBSA | - | Pattern Based Bits Shuffling |
| PDE | - | partial difference equation |
| PND | - | Random |
| PoV | - | Pairs of Values |
| PSNR | - | Peak Signal-to-Noise Ratio |
| PSO | - | Particle Swarm Optimization |
| PVD | - | Pixel Value Differencing |
| RGB | - | Red, Green and Blue |
| ROP | - | Region of Interest |
| RPE | - | Random Pixel Embedding |
| SIPI | - | Signal and Image Processing Institute |
| SIS | - | Steganography Image System |
| SSIM | - | Structural Similarity Index |
| TNA | - | Triple Number Approach |
| TCP/IP | - | Transmission Control Protocol/Internet Protocol |
| TES | - | Triple Embedding Scheme |
| TTCS | - | Triple Text Coding Scheme |
| UTM | - | Universiti Teknologi Malaysia |
| W | - | Words |
| WFFT | - | Weight Fractional Fourier Transform |
| WT | - | Wavelet Transform |

## LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

In recent times, the fast development of the information and communication technology enabled the free and easy transfer of the vast amount of data over the open internet. This free flow of massive data over the internet network in turn posed severe threat towards the privacy preserved sensitive data transfer where the intruders/attackers are constantly faced. Although the transfer (sending or receiving) of the data information (such as the video, audio, image, and text) became very easy, securing the sensitive information over the insecure public network posed new challenges. For secured information transfer from the sender to received end, diverse information hiding techniques including the steganography, cryptography and watermarking have been introduced. Using the steganography scheme, the secret or private data can be hidden within different media including the colour or grayscale image (Singh et al., 2019).

The steganography technique can be categorized into various types based on the cover media such as the image, audio, text, video, DNA, or even protocol (Hussain et al. 2018) wherein every such cover media has its own merits and demerits (Dhar and Banerjee 2019; Kadhim et al., 2019). Over the past decades, intensive studies have been performed to develop some highly robust and secured image steganography schemes (ISSs). Essentially, these ISSs became promising owing to their easy transmission capacity of the multimedia contents via different low-cost devices (for example smart mobile phones and IP digital cameras) and social media application platforms such as the WhatsApp, Twitter, Facebook and LinkedIn (Hussain et al., 2018). Despite the popularity and robustness of these ISSs, various issues related to the image security and concealment of the secret message for the safe information transfer remains unresolved. In addition, a better understanding of the secret data embedding processes in an image is vital for the development of an outperforming ISS (Sahu and Swain, 2020).

Generally, the steganography schemes are attained in the spatial and transform domains (Hussain et al., 2018; Kadhim et al., 2019). Two important concepts are involved in the steganography technique so called stego and cover image. A stego image hosts the secret information with certain quality, whereas the cover image is the pure image without containing any secret information within it and is ready to host the secret information.

The significance of the steganography scheme relies on the security of the secret message that is embedded within the image. However, the problems arise when the illegal messages or data embedded by the unauthorized users become expansive (Amritha et al., 2016; Li et al., 2011). In the steganography technique, the sender and receiver work together to hide the data needs to be transferred and then extracted. In this process, the sender hides the message and delivers, while the receiver extracts the information hidden in the stego image using a stego key (Seyyedi et al., 2016).

The steganography technique has been applied in the field of medical diagnoses (Arunkumar et al., 2019; Eze et al., 2019), military and defense (Tuncer and Avci, 2016), multimedia biometric data security (Mohsin et al., 2018) and cloud computing (Shanthakumari and Malliga, 2019). The fundamental issues and difficulties concerning the performance of the existing state-of-the-art steganography schemes are related to the payload capacity, imperceptibility, and security (Hussain et al., 2018) as indicated in Figure 1.1.

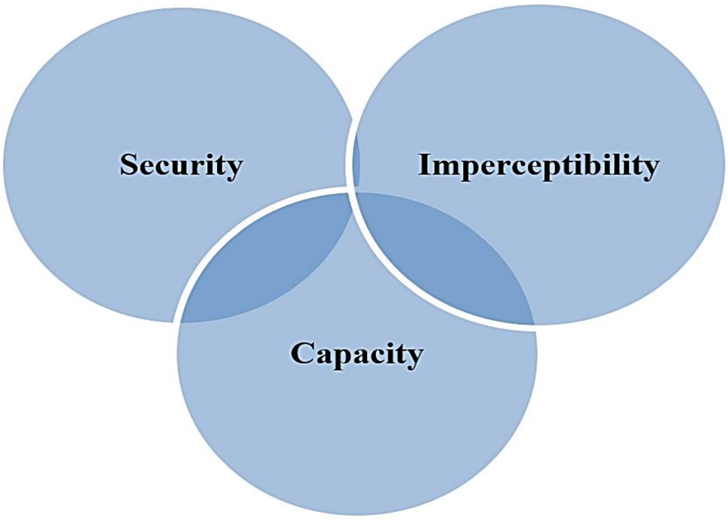


Figure 1.1 Three main performance criteria concerning the existing steganography schemes.

The payload capacity of a steganography system is defined as the maximum size of the secret message that can be hidden into the image media (Kadhim et al., 2019). The maximum payload refers to the highest limit of the secret data that can be embedded into the image. The imperceptibility of a steganography system signifies the carrier media quality that can be used for hiding the secret message following the algorithm embedment (Hussain et al., 2018). The security of a steganography system (Swain et al., 2019) refers to its robustness against various statistical attacks such as the chi-square, human visual system (HVS) and histogram analysis. In this perception, present study intends to resolve various issues related to the existing steganography system and improve its robustness in terms of high security, high payload capacity, and imperceptibility.

## 1.2 Problem Background

Intensive efforts have recently been made to secure the secret data by hiding it within the transmitting image media, making the secret data unnoticeable to the intruders (Wang et al., 2019; Kadhim et al., 2019). Consequently, the steganography approach for the data hiding in the image media received immense attention in the field of security and privacy preserved information communications (Yeung et al., 2019). Conversely, the use of other transmission media such as the protocols and text are quitted sparse (Yeung et al., 2019). As aforementioned, the imperceptibility (embedding method), security and payload capacity being the main concerns related to the steganography system's performance need further improvement (Hussain et al., 2018; Kadhim et al., 2019).

It is important to mention that several studies in the image steganography and steganalysis focused on the improvement of the imperceptibility (embedding method). Based on this fact, the performance of the developed image steganography system was assessed in terms of the measures including the peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) (Vikranth et al., 2015; Rai et al., 2015). Actually, the enhancement of the PSNR and SSIM became one of the main challenges in the steganography techniques. The payload capacity being a trade-off between the PSNR and SSIM, different approaches have been proposed to enhance the PSNR and SSIM values. Despite the accomplishment of some encouraging results, only a few investigations have been conducted on the payload capacity (Shyla et al.,2019; Raeiatibanadkooki et al., 2016). In-depth literature survey indicated that the studies on the trade-off between the steganography performance criteria are unbalanced (Zhang et al., 2019; Yiannakou et al., 2016). Some researchers used a low payload capacity in order to increase PSNR and SSIM values. It has been observed that the use of the high payload capacity can affect the image quality, reducing the PSNR plus SSIM and vice versa. The PSNR is considered as low if it is less than equal to 45 dB. Conversely, the PSNR is acceptable if it is less than equal to 59 dB, otherwise, PSNR is regarded as high (AbdelQader et al., 2017). In the case of SSIM, two images are said to be similar to each other if the value of SSIM is equal to 1. Otherwise, the images are considered to be noisy (Kadhim et al., 2019; Yeung et al., 2019).

Hegde et al. and Srinivasan et al. (2018) obtained the enhanced PSNR values of 68.25 and 67.23 dB, respectively. They manipulated the payload capacity (low capacity) in order to get improved PSNR values with better security. Seyyedi et al. (2016) proposed a method based on the wavelet coefficients and Rivest Cipher (RC4) encryption technique. It made the method robust against the Chi-square attack and produced better PSNR of 65.09 and SSIM of 0.9876, however with a low payload capacity of 16384 bytes. Jumanto (2018) developed an image steganography method based on the canny edge detection and sobel filter wherein the implementation of the algorithm for the embedding and extracting processes was easy. Although, the method failed to achieve a better PSNR value (42.36), the results for the payload capacity was acceptable (25655 bytes).

Sari et al. (2019) proposed a technique using the Data Encryption Standard (T-DES) to encrypt the data before embedding where bit selection was made for encoding the secret message. In this method, the most significant bit (MSB) was used to trick the hacker with the inverted least significant bit (LSB) order. The payload capacity (16384 bytes) was manipulated to attain the acceptable values of the PSNR (52.32) and SSIM (0.9790). Hasanzadeh and Shokranipour (2019) used the Particle Swarm Optimization (PSO) method to obtain a high PSNR value. This method achieved an acceptable payload capacity (24880 bytes) and better SSIM (0.9989) with PSNR of 64.11 compared to other methods. Duan et al. (2020) introduced a new method based on the deep learning to enhance the payload capacity. First, the discrete cosine transforms (DCT) was employed to transform the secret image. Next, the transformed secret message was encrypted using the elliptic curve cryptography (ECC). The proposed method showed better performance in terms of the payload capacity but failed to achieve high PSNR (43.13) and SSIM (0.9683).

Numerous methods have been proposed to hide the information within an image for improving the imperceptibility (embedding scheme). In terms of the imperceptibility and PSNR results, (Hegde et al., 2015; Srinivasan et al., 2015) proposed better methods so far. However, the results are not optimum yet due to the presence of noise within the stego image compared to the original one. Meanwhile, all the proposed approaches in the spatial domain (Kini and Kini 2019; Kadhim et al., 2019) used a binary impact value ($2^n$) to hide the secret bits (0 or 1). The binary impact value has various limitations such as the (i) consumption of more space for the embedding algorithm that leads to less payload capacity and less imperceptibility; (ii) normal coding strength in the binary impact value that is easy to hack because of the awareness of the statistical attack to work with the binary impact values and their subsequent direct analyses. This in turn affects the security and robustness of the methods. According to Swain et al. (2019), a robust steganography technique must be able to recover the secret message after exposed to a number of potential attacks that are available for different benchmarking techniques including the chi-Square, HVS, and Histogram analysis. Huang et al. (2019) stated that the security is one of the noticeable features and very important for the steganography method. In fact, there exists different evaluation performance software such as Chi-square.

To achieve the improved security in the steganography method different strategies have been adopted. Amongst all these approaches, the pixel randomization was shown to be the most suitable one because it shares the same pixel features (Lynnyk, 2010). Several approaches have recently been introduced to increase the security including the image partitioning and pixel randomization. Although these proposed approaches are promising, each of them encounters different limitations during the performance evaluation. For instance, Das et al. (2018) proposed an image steganography algorithm based on the pixel intensity and randomization of different pixel values to achieve improved security. In this method, greater space and manipulation of the pixels order in the stego image were considered wherein the secret bits were hold in two bits of the LSB. The proposed algorithm was simple in terms of the embedding process and the performance was evaluated in terms of the PSNR and Chi-square attack. The poor performance of the method against Chi-square attack was due to the use of one partitioning for an image.

The issues concerning the security performance of the image steganography have widely been discussed in the recent state-of-the-art literatures. Despite the development of different approaches to resolve these issues, the weaknesses of the image steganography still persists. Due to easy access of the information, the attackers acquired enough knowledge and expertise in the field of security, thus can breach the secret codes and keys. The intruders/hackers/attackers can anticipate easily the greater security of the secret data in the images due to the abundance of the steganalysis methods and tools with improved performance. Therefore, finding the newer and powerful approaches for the secret data concealing became necessary. It is inferred that the new approaches may enable in securing the transmitted information between two parties (Amritha et al., 2016).

The LSB is one of the spatial domain techniques that are used by different approaches. However, this technique has some weaknesses (low security and poor robustness) against the statistical attack. This weakness can be attributed to the direct embedding in the LSB part of the pixel. The statistical attack is based on analyzing the LSB directly because of the presence of the secret data in this part. In order to enhance the security, some researchers have worked on the frequency domain transformation. The use of DCT and discrete wavelength transform (DWT) was shown to produce better results (Saidi et al., 2019; Sharma et al., 2019). These frequency-domain techniques indicated stronger security than the LSB-based technique when applied against the Human Visual System (HVS) and Histogram analysis attacks.  However, these methods have limitations when applied against other attacks such as the chi-square attack because this domain uses coefficients directly to embed the secret message. In addition, the chi-square is influenced by the slightest effects with the coefficients inside the image, thereby affecting the security.

The existing steganography schemes use additional tools such as the the compression, noise removal or encryption in advance to increase the data security. However, the inclusion of such extra tools affects various other details of the developed steganography scheme, thereby increasing its complexity and execution time. Despite some intriguing applications of the steganography schemes in the biometric and medical fields, many issues involving these applications require further improvement (Meng et al., 2019). In addition, these applications suffer from the security problems which need to be enhanced (Douglas et al., 2019). To reduce the complexity of the image steganography system, the tunable visual image quality-based genetic algorithm (GA) was introduced by Kanan and Nazeri (2014), wherein the lossless data in the spatial domain was utilized for the problems optimization. Experimental results showed a high embedded capacity with enhanced PSNR. However, the system performance was poor against the statistical attacks which were due to the information hiding using a single randomized stage. Meanwhile, Pandian et al. (2017) used the DWT for the medical images upon enhancement. In addition, the de-noising processes were used with increasing PSNR following the LSB substitution. The results revealed an enhancement in the security with the decrease in the payload capacity.

In an image steganography system, the word *security* is considered as a vital evaluation parameter. Indirectly, security refers to the undetectability or un-noticeability of the hidden data information. Therefore, any steganography system is regarded as highly secure if the secret data remains undetectable by the statistical analysis or attackers. In fact, the security issue needs to be resolved for avoiding the illegitimate data access by the intruders while transmitting through an insecure communication channel. Generally, the steganography systems may suffer from different types of the steganalysis detection attacks. The intruders are attracted to trace the existence or even to retrieve the secret data bits from the stego images. It is worth noting that no single steganography system is immune to all kinds of the statistical attacks. Thus, all steganography system used one or two statistical attacks during their performance evaluation (Rawat et al., 2020). Qian et al. (2018) suggested a better steganography approach to conceal the data for better security wherein the pixel difference histogram (PDH) was used during the data transmission. The performance of the proposed steganography approach was evaluated against chi-square attack only. Ebrahim et al. (2017) achieved excellent security performance for the data hiding using an encryption algorithm wherein secret text was encrypted before the embedding process. The HVS and histogram analysis was used to evaluate the proposed steganography system performance against attacks. In spite of all such developments, achieving the enhanced security in the image steganography system remains challenging.

The maximum payload capacity of a steganography system refers the highest size of the secret message to be hidden in the media file such as image, video, or audio subjected to a specific condition. Thus, it is desirable to increase payload capacity of a steganography system for achieving better performance. In other words, an efficient image steganography system aims to send the maximum amount of data using the minimum pixels in the cover media. A significant change in the multimedia file is observed when the maximum data limit is exceeded, causing a failure of the steganography algorithm. The steganography payload is measured using the data hiding ratio (DHR) which is defined as the ratio between the maximum payload capacities to the original media size (Das et al., 2018). Abraham et al. (2004) defined the embedding rate as the payload capacity amount of data hidden (in bits) relative to the original image size. Thus, keeping the higher payload capacity in a steganography system without sacrificing the imperceptibility and security is a major challenge (Jawad et al., 2019). The size of the payload capacity is characterized in terms of the bits per pixel (Bpp), bytes and percentage (%). Table 1.1 shows the low, moderate, and high payload capacity used in different steganography systems (Hussain et al., 2018; Kadhim et al., 2019).

Table 1.1 The payload capacity used in various steganography system

| Payload capacity | Low capacity | Moderate capacity | High capacity |
|---|---|---|---|
| Bytes | ≤ 16384 | ≤ 49152 | > 49152 |
| Bpp | ≤ 0.5 | ≤ 1.5 | > 1.5 |
| Percentage (%) | ≤ 6.25% | ≤ 18.75% | > 18.75% |

Most of the steganography systems employ the compression algorithms to condense the secret data before embedding. The compression algorithms increase the secret data amount inside an image. Huffman coding is the most common approach used in the compression process which can compress the secret data more than 30%. The coding has widely been used to solve the payload capacity problems in the steganography system, wherein the secret data is compressed prior to its insertion into an image (Sun, 2016). The noise level in the cover image increases with the increase of the payload capacity in the cover image, making it easy for the intruder to notice and analyze the secret message. Therefore, the approach used for the performance evaluation of any steganography system must aim to carry out the statistical analysis for the embedded data. To achieve this goal, numerous approaches employ LSB for embedding the secret bit into a pixel. However, the LSB is limited as insertion is restricted to one or two bits to host the data, leading to a major weakness of the steganography system. When the capacity of the stego images (images that hold the secret message) increases, the images become more susceptible to various types of attacks. The chi-square ($\chi^2$) attack is very sensitive to the amount of data embedded into an image (capacity) (Al-Dmour and Al-Ani, 2016). The HVS attack is very sensitive to the LSB change in the image pixels that reveal the secret message position (Yahya, 2019), which.

Saeed et al. (2020) and Mohammed et al. (2016) used different LSB approaches in the steganography system and obtained a moderate payload capacity of 32768 and 32768 bytes, respectively. However, the proposed system ignored the imperceptibility, indicating an easy detection of the secret data by the intruders. Additionally, the payload capacity was based on the structure of the given image. Better types of images that possess a high concealing capacity are characterized by the high contrast ratio in the pixel values (Das et al., 2018). Unlike the previous study (Hasanzadeh et al., 2019), Gaurav and Ghanekar (2018) used some parts of the images like the edge. Al-Dmour,and Al-Ani (2015) utilized high contrast of pixels and Yang et al. (2018) the specific region of interest (ROI) area to enhance the performance of the steganography system. Overall, an increase in the payload capacity of the secret message involves very careful execution and constant monitoring to achieve a balance between the security and imperceptibility. Briefly, the implementation of a novel suitable impact value may be helpful in terms of the payload capacity, security, and imperceptibility of the outperforming steganography system.

## 1.3 Problem Statement

The existing image steganography systems have various limitations that need to be surmounted. First, the challenging issue related to the payload capacity of the image needs to be resolved because any fault in the image steganography approach can affect the payload capacity. Commonly, the compression algorithms are used to reduce the secret message size via the condensation process. In addition, the compression approach changes the features of secret messages. The existing compression methods are easy to analyse using steganalysis and decompression tools. Therefore, changing the secret messages features and transform it into a new form is helpful to payload capacity and security as well.

Second, the weak security performance of the existing steganography method against various statistical attacks is the major shortcoming that needs to be overcome. The majority of the previous studies used an image partitioning strategy with the single randomization of the bocks and pixels to improve the security of the developed steganography system (Tuncer et al., 2016; Sahu et al. 2019; Heidari et al., 2019). However, such a strategy produces the stego images that are easily detectable via statistical analysis such as the chi-square attack, thereby making the steganography system insecure against attacks. This clearly indicates that the challenges to re-arrange the image pixels inside a certain image to enhance the pixels location integrity still an open problem that needs in-depth understanding.

The Third challenging issue in steganography is imperceptibility, which is measured via the Peak Signal to Noise Ratio (PSNR) equation. The high PSNR signifies better imperceptibility of the image, indicating a better steganography system (Hussain et al., 2018). The PSNR equation is based on the altering Mean Square Error (MSE) values wherein the solutions suffer from a high rate of MSE that reduces the PSNR of the stego image (Duan et al., 2020; Sari et al., 2019). Thus, it is essential to resolve this issue by reducing the MSE, thereby improving the imperceptibility of the stego image. In short, despite the substantial research efforts, the development of a robust steganography system that overcomes the problems involving the security, payload capacity, and imperceptibility of the stego image is still lacking.

## 1.4 Research Aims

The main aim of this study is to introduce an enhanced image steganography scheme by expanding the payload capacity and increased imperceptibility for secures the secret data inside an image.

## 1.5 Objectives

Based on the aforementioned research gaps the following objectives are set:

i. To propose a new method for expanding the payload capacity with changing secret bits stream values and compressed secret text inside an image.

ii. To propose a new method for partitioning the image with a random pixel selection to improve the security of image steganography.

iii. To introduce a new embedding method based on the suitable impact value for keeping the high imperceptibility.

## 1.6 Scope of the Study

This proposed research tries to improve image steganography scheme. Therefore, in order to achieve the desired goals and objectives of the proposed research, it is very important to define the research scope, which can be explained by the following points:

i. Text file is used to embed secret message into an image by considering the proposed condition of the steganography scheme.

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

iii. Signal and Image Processing Institute (SIPI) is the dataset that will be used to carry out experiments on the proposed scheme. The images are in the size of 512 x 512 pixels. This dataset contains images that are suitable to implement the proposed scheme.

iv. The performance of the system is evaluated by implementing different analysis methods such as Chi-Square attack, Human Visual System (HVS) attack, structural similarity index measure (SSIM), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

## 1.7 Motivation

The study develops a steganography approach in the image due to the images are excellent media that exhibit great redundancy in their representation. In addition, the usage of images is widespread in organizations to communicate among their members. Apart from that, images are also used extensively for communication between members of the military, intelligence operatives, agents of companies, and medical staff to hide sensitive or vital data. Moreover, a steady increase in malicious attacks on industrial applications, private applications, business, and sensitive government documents by adversaries of various kinds have motivated researchers and developers in the information security field to seek technical solutions to protect the privacy of documents sent over communication channels.

The present work is motivated by the need for a more secure solution for protecting secret data that is being transmitted over communication channels so as to strengthen the privacy and integrity of the secret data.

## 1.8 Significance of the Study

The proposed scheme could overcome some of the limitations associated with the existing steganography system. The newly developed system is anticipated to be more reliable in terms of security and capacity. Security of the steganography scheme is expected to be enhanced while keeping the PSNR score at a high level. This study anticipates challenges in the aspect of capacity and would attempt to lower its dependency. Limitations suffered by existing approaches in the embedding process are overcome by using the proposed scheme. Meanwhile, the performance evaluation results of the present steganography system are showed improved capacity and security. The designed steganography system may contribute to several applied fields of data communication such as the military, medical, cloud computing, and industry where high security and robustness are a priority.

Contributions of the study are not only limited to implementation in the field of image steganography, as the proposed scheme may also be used in other sections of steganography, watermarking, and encryption fields. The proposed scheme proposes ideal quality in terms of randomness criteria, and this could make the proposed work applicable in fields that require randomness such as a complete randomised design, computer simulation, statistical sampling, and in fields where unpredictable sequences are desired.

## 1.9 Thesis Outline

The proposed research is presented through this thesis and organized into seven chapters, which can be outlined as follows:

**Chapter 1:** An introduction to the proposed research is elaborated including problem formulation and a description of a research goal, objectives, scope, and significance.

**Chapter 2:** The chapter introduces hiding data approaches in a critical manner, research gaps, and principles in the classification of steganography are discussed in detail. The advantages and weaknesses of existing approaches were elaborated as well.

**Chapter 3:** General research framework, datasets used in the system testing and training, and the techniques used to evaluate the system are presented.

**Chapter 4:** The Triple number approach with the main contributions of the proposed scheme is described in more detail in this chapter.

**Chapter 5:** The proposed Triple number image steganography scheme is introduced and described in detail.

**Chapter 6:** Performance evaluation and security attacks of proposed scheme are explained in this chapter.

**Chapter 7:** Contributions and future works of the proposed research are elaborated in this chapter.

## REFERENCES


Abd-El-Atty, B., Iliyasu, A. M., Alaskar, H., El-Latif, A., & Ahmed, A. (2020). A Robust Quasi-Quantum Walks-Based Steganography Protocol for Secure Transmission of Images on Cloud-Based E-healthcare Platforms. *Sensors*, *20*(11), 3108.

Agrawal, S., and Kumar, M. (2016). An Improved Reversible Data Hiding Technique Based on Histogram Bin Shifting. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics* (pp. 239-248). Springer India.

Ahmad, P. M. T. (2019). Digital Image Information Hiding Methods for Protecting Transmitted Data: A Survey. *Journal of Communications*, *14*(1).

Akhtar, N. (2016). An Efficient Lossless Modulus Function Based Data Hiding Method. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics* (pp. 281-287). Springer India.

Al-Ataby, A., and Al-Naima, F. (2008). A modified high capacity image steganography technique based on wavelet transform. *changes*, 4, 6.

Al-Dmour, H., and Al-Ani, A. (2016). A steganography embedding method based on edge identification and XOR coding. *Expert Systems with Applications*, 46, 293-306.

Al-Tamimi, A. G. T., and Alqobaty, A. A. (2015). Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm. *International Journal of Computer Science and Information Security*, 13(1), 1.

AlKhodaidi, T., & Gutub, A. (2020). Refining image steganography distribution for higher security multimedia counting-based secret-sharing. *Multimedia Tools and Applications*, 1-31.

Akhtar, N., Khan, S., & Johri, P. (2014, February). An improved inverted LSB image steganography. In *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)* (pp. 749-755). IEEE.

Amritha, P. P., Induja, K., and Rajeev, K. (2016). Active Warden Attack on Steganography Using Prewitt Filter. In Proceedings of the International Conference on Soft Computing Systems (pp. 591-599). Springer India.

Amritha, P. P., Muraleedharan, M. S., Rajeev, K., and Sethumadhavan, M. (2016). Steganalysis of LSB Using Energy Function. In *Intelligent Systems Technologies and Applications* (pp. 549-558). Springer International Publishing.

Anandkumar, R., & Kalpana, R. (2019). Designing a fast image encryption scheme using fractal function and 3D Henon Map. *Journal of Information Security and Applications*, *49*, 102390.

Anandpara, D., and Kothari, A. (2015). Working and Comparative Analysis of Various Spatial Based Image Steganography Techniques. *International Journal of Computer Applications*, *113*(12), 8-12.

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.

Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. *IETE Technical Review*, *30*(4), 344-358.

Baig, F., Khan, M. F., Beg, S., Shah, T., and Saleem, K. (2016). Onion steganography: a novel layering approach. *Nonlinear Dynamics*, 1-16.

Bao, Z., Guo, Y., Li, X., Zhang, Y., Xu, M., & Luo, X. (2019). A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. *Journal of Ambient Intelligence and Humanized Computing*, 1-13.

Barr, K. C., and Asanović, K. (2006). Energy-aware lossless data compression. ACM Transactions on Computer Systems (TOCS), 24(3), 250-291.

Bhardwaj, R., & Sharma, V. (2016). Image steganography based on complemented message and inverted bit LSB substitution. Procedia Computer Science, 93, 832-838.

Bhatt, S., Ray, A., Ghosh, A., and Ray, A. (2015, January). Image steganography and visible watermarking using LSB extraction technique. In*Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on* (pp. 1-6). IEEE.

Bhattacharya, D., Chakraborty, S., Roy, P., Kairi, A., and IEM, K. (2015). An Advanced Dictionary Based Lossless Compression Technique for English Text Data. *Biometrics and Bioinformatics*, *7*(1), 4-11.

Benedicks, M., & Carleson, L. (1991). The dynamics of the Hénon map. *Annals of Mathematics*, *133*(1), 73-169.

Bilal, M., Imtiaz, S., Abdul, W., & Ghouzali, S. (2013, May). Zero-steganography using dct and spatial domain. In *2013 ACS International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-7). IEEE.

Birajdar, G. K., Vyawahare, V. A., & Patil, M. D. (2018). Secure and Robust ECG Steganography Using Fractional Fourier Transform. *Cryptographic and Information Security Approaches for Images and Videos*, 19.

Böhme, R. (2010). Principles of Modern Steganography and Steganalysis. In*Advanced Statistical Steganalysis* (pp. 11-77). Springer Berlin Heidelberg.

Botta, M., Cavagnino, D., and Pomponiu, V. (2016). A modular framework for color image watermarking. *Signal Processing*, *119*, 102-114.

Bower, A., Insoft, R., Li, S., Miller, S. J., and Tosteson, P. (2015). The distribution of gaps between summands in generalized Zeckendorf decompositions. *Journal of Combinatorial Theory, Series A*, *135*, 130-160.

Bucerzan, D., and Raţiu, C. (2016). Image Processing with Android Steganography. In *Soft Computing Applications* (pp. 27-36). Springer International Publishing.

Budiman, G., and Novamizanti, L. (2015). White Space steganography On Text By Using lzw-Huffman Double Compression.*International Journal of Computer Networks and Communications*, *7*(2), 136A.

Chakravarthy, S., Sharon, V., Balasubramanian, K., and Vaithiyanathan, V. (2016). Art of Misdirection Using AES, Bi-layer Steganography and Novel King-Knight's Tour Algorithm. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 97-108). Springer International Publishing.

Chandran, S., and Bhattacharyya, K. (2015, January). Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography. In Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on (pp. 1-5). IEEE.

Chang, C. C., Chen, T. S., and Chung, L. Z. (2002). A steganographic method based upon JPEG and quantization table modification. *Information Sciences*,*141*(1), 123-138.

Channalli, S., and Jadhav, A. (2009). Steganography an art of hiding data. *arXiv preprint arXiv:0912.2319*.

Charbal, A., Dufour, J. E., Guery, A., Hild, F., Roux, S., Vincent, L., and Poncelet, M. (2016). Integrated Digital Image Correlation considering gray level and blur variations: Application to distortion measurements of IR camera. *Optics and Lasers in Engineering*, *78*, 75-85.

Chary, A. S. (2016). Invisible Image Watermarking Using Hybrid DWT Compression-Decompression Technique. *International Journal of Advanced Research Foundation*, *3*(1).

Chen, P. Y., and Lin, H. J. (2006). A DWT based approach for image steganography. *International Journal of Applied Science and Engineering*,*4*(3), 275-290.

Chowdhuri, P., Jana, B., & Giri, D. (2018). Secured steganographic scheme for highly compressed color image using weighted matrix through DCT. *International Journal of Computers and Applications*, 1-12.

Das, P., Kushwaha, S. C., and Chakraborty, M. (2015, February). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on* (pp. 845-849). IEEE.

Das, S. K., and Dhara, B. C. (2015, April). An Image Secret Sharing Technique with Block Based Image Coding. *In Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on* (pp. 648-652). IEEE.

Das, S., Sharma, S., Bakshi, S., & Mukherjee, I. (2018). A framework for pixel intensity modulation based image steganography. In Progress in Advanced Computing and Intelligent Engineering (pp. 3-14). Springer, Singapore.

Dhar, M., & Banerjee, S. (2019). An Efficient and Enhanced Mechanism for Message Hiding Based on Image Steganography Using. *Advances in Communication, Devices and Networking: Proceedings of ICCDN 2018*, 537, 461.

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications*, *77*(13), 17333-17373.

Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network. *IEEE Access*, *8*, 25777-25788.

El_Rahman, S. A. (2018). A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. *Computers & Electrical Engineering, 70*, 380-399.

El-Emam, N. N., and Al-Diabat, M. (2015). A novel algorithm for colour image steganography using a new intelligent technique based on three phases. *Applied Soft Computing, 37*, 830-846.

EL-Latif, A. A. A., Abd-El-Atty, B., & Venegas-Andraca, S. E. (2019). A novel image steganography technique based on quantum substitution boxes. *Optics & Laser Technology, 116*, 92-102.

Eze, P., Parampalli, U., Evans, R., & Liu, D. (2019, June). Integrity Verification in Medical Image Retrieval Systems using Spread Spectrum Steganography. In *Proceedings of the 2019 on International Conference on Multimedia Retrieval* (pp. 53-57). ACM.

Farrag, S., & Alexan, W. (2019, April). Secure 2D Image Steganography Using Recamán's Sequence. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-6). IEEE.

Fathimal, P. M., and Rani, P. A. J. (2016). K Out of N Secret Sharing Scheme with Steganography and Authentication. In *Computational Intelligence, Cyber Security and Computational Models* (pp. 413-425). Springer Singapore.

Fridrich, J., and Goljan, M. (2003, June). Digital image steganography using stochastic modulation. In *Electronic Imaging 2003* (pp. 191-202). International Society for Optics and Photonics.

Fridrich, J., Goljan, M., and Du, R. (2001, October). Reliable detection of LSB steganography in color and grayscale images. In *Proceedings of the 2001 workshop on Multimedia and security: new challenges* (pp. 27-30). ACM.

Ghasemi, E., Shanbehzadeh, J., and Fassihi, N. (2011, March). High capacity image steganography using wavelet transform and genetic algorithm. In*Proceedings of the international multiconference of engineers and computer scientists* (Vol. 1).

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

Ghosh, D., Chattopadhyay, A. K., & Nag, A. (2019). A Novel Approach of Image Steganography with Encoding and Location Selection. In *Proceedings of*

*International Ethical Hacking Conference 2018* (pp. 115-124). Springer, Singapore.

Georges, J., & Magdi, D. A. (2020). Using Artificial Intelligence Approaches for Image Steganography: A Review. In *Internet of Things—Applications and Future* (pp. 239-247). Springer, Singapore.

Gupta, J. (2015). A Review on Steganography techniques and methods. International Society for Optics and Photonics, *vol*, *1*, 1-4..

Gupta, P., & Bhagat, J. (2019). Image Steganography Using LSB Substitution Facilitated by Shared Password. In *International Conference on Innovative Computing and Communications* (pp. 369-376). Springer, Singapore.

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

Gutub, A., Al-Qahtani, A., & Tabakh, A. (2009, May). Triple-A: Secure RGB image steganography based on randomization. In *2009 IEEE/ACS International Conference on Computer Systems and Applications* (pp. 400-403). IEEE.

Shokranipour, S., & Hasanzadeh, M. (2016). High capacity image steganography method by using Particle Swarm Optimization. *The Modares Journal of Electrical Engineering*, *15*(4), 1-7.

Hegde, R. and Jagadeesha S., 2015 "Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique". *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume: 3 Issue: 7.

Heidari, S., Abutalib, M. M., Alkhambashi, M., Farouk, A., & Naseri, M. (2019). A new general model for quantum image histogram (QIH). *Quantum Information Processing*, *18*(6), 175.

Herrigel, A., Voloshynovskiy, S. V., and Hrytskiv, Z. D. (2000, June). Optical/digital identification/verification system based on digital watermarking technology. In *International Workshop on Optoelectronic and Hybrid Optical/Digital Systems for Image/Signal Processing* (pp. 170-176). International Society for Optics and Photonics.

Holub, V., and Fridrich, J. (2013, June). Digital image steganography using universal distortion. In *Proceedings of the first ACM workshop on Information hiding and multimedia security* (pp. 59-68). ACM.

Hu, WenWen, Ri-Gui Zhou, and YaoChong Li. "Quantum Watermarking Based on Neighbor Mean Interpolation and LSB Steganography Algorithms." *International Journal of Theoretical Physics* (2019): 1-24.

Huang, C. W., Chou, C., Chiu, Y. C., & Chang, C. Y. (2018). Embedded FPGA Design for Optimal Pixel Adjustment Process of Image Steganography. *Mathematical Problems in Engineering*, *2018*.

Huang, F., and Kim, H. J. (2016). Framework for improving the security performance of ordinary distortion functions of JPEG steganography. *Multimedia Tools and Applications*, 75(1), 281-296.

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

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66.

Huynh-The, T., Hua, C. H., Tu, N. A., Hur, T., Bang, J., Kim, D., ... & Lee, S. (2018). Selective bit embedding scheme for robust blind color image watermarking. *Information Sciences*, *426*, 1-18.

Ibrahim, R., and Kuan, T. S. (2011). Steganography algorithm to hide secret message inside an image. *arXiv preprint arXiv:1112.2809*.

Islam, Ammad Ul, *et al*. "An improved image steganography technique based on MSB using bit differencing." *2016 Sixth International Conference on Innovative Computing Technology (INTECH). IEEE*, 2016.

Islam, M. N., Islam, M. F., and Shahrabi, K. (2015). Robust information security system using steganography, orthogonal code and joint transform correlation. *Optik-International Journal for Light and Electron Optics*, *126*(23), 4026-4031.

Jain, N., Meshram, S., and Dubey, S. (2012). Image Steganography Using LSB and Edge–Detection Technique. *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, *223*.

Jana, B., Giri, D., and Mondal, S. K. (2016). Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion. *International Journal of Network Security*, *18*(4), 633-643.

Jero, S. E., and Ramu, P. (2016). Curvelets-based ECG steganography for data security. *Electronics Letters*, *52*(4), 283-285.

Jiang, N., Dong, X., Hu, H., Ji, Z., & Zhang, W. (2019). Quantum Image Encryption Based on Henon Mapping. *International Journal of Theoretical Physics*, 1-13.

Jiang, N., Zhao, N., and Wang, L. (2016). Lsb based quantum image steganography algorithm. *International Journal of Theoretical Physics*, *55*(1), 107-123.

Johnson, N. F., and Jajodia, S. (1998, January). Steganalysis of images created using current steganography software. In *Information Hiding* (pp. 273-289). Springer Berlin Heidelberg.

Joshi, K., Yadav, R., & Chawla, G. (2017). An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography. *International Journal of Engineering and Technology (IJET)*, *9*(4), 143.

Jumanto, J. (2018). An enhanced LSB-image steganography using the hybrid Canny-Sobel edge detection. *Cybernetics and Information Technologies*, 18(2), 74-88.

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.

Kanan, H. R., and Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert Systems with Applications*, *41*(14), 6123-6130.

Kaur, A., Dhir, R., and Sikka, G. (2010). A new image steganography based on first component alteration technique. *arXiv preprint arXiv:1001.1972*.

Khan, S., Ahmad, N., and Wahid, M. (2016). Varying index varying bits substitution algorithm for the implementation of VLSB steganography.*Journal of the Chinese Institute of Engineers*, *39*(1), 101-109.

Kim, C., Yun, S., Jung, S. W., and Won, C. S. (2016). Color and Depth Image Correspondence for Kinect v2. In *Advanced Multimedia and Ubiquitous Engineering* (pp. 333-340). Springer Berlin Heidelberg.

Kim, J., Park, H., & Park, J. I. (2020). CNN-based image steganalysis using additional data embedding. Multimedia Tools and Applications, 79(1-2), 1355-1372.

Kini, N. G., & Kini, V. G. (2019). A Parallel Algorithm to Hide an Image in an Image for Secured Steganography. In *Integrated Intelligent Computing, Communication and Security* (pp. 585-594). Springer, Singapore.

Kini, N. G., & Kini, V. G. (2019). A Secured Steganography Algorithm for Hiding an Image in an Image. In Integrated Intelligent Computing, Communication and Security (pp. 539-546). Springer, Singapore.

Knapp, J. F., and Worrell, S. W. (2015). *U.S. Patent No. 9,002,134*. Washington, DC: U.S. Patent and Trademark Office.

Kolakalur, A., Kagalidis, I., and Vuksanovic, B. (2016). Wavelet Based Color Video Steganography. *International Journal of Engineering and Technology*,*8*(3), 165.

Kumar, A., Ghrera, S. P., and Tyagi, V. (2016). Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis. *Indian Journal of Science and Technology*, *8*(35).

Kumar, N. (2016). Steganographic Methods: A Survey on Novel Approaches.*International Journal Of Computer Science And Interdisciplinary Research*, *1*(1).

Kuo, W. C., Chang, S. Y., Wang, C. C., and Chang, C. C. (2016). Secure multi-group data hiding based on gemd map. *Multimedia Tools and Applications*, 1-19.

Kuo, W. C., Wang, C. C., and Hou, H. C. (2016). Signed digit data hiding scheme. *Information Processing Letters*, *116*(2), 183-191.

Laha, S., and Roy, R. (2015, December). An improved image steganography scheme with high visual image quality. *In Computing, Communication and Security (ICCCS), 2015 International Conference on* (pp. 1-6). IEEE.

Lee, K. D., and Hubbard, S. (2015). Heuristic Search. In *Data Structures and Algorithms with Python* (pp. 281-297). Springer International Publishing.

Lee, Y. K., and Chen, L. H. (2000, June). High capacity image steganographic model. In *Vision, Image and Signal Processing, IEE Proceedings* (Vol. 147, No. 3, pp. 288-294). IET.

Li, B., He, J., Huang, J., and Shi, Y. Q. (2011). A survey on image steganography and steganalysis.Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172.

Liao, X., Yu, Y., Li, B., Li, Z., & Qin, Z. (2019). A New Payload Partition Strategy in Color Image Steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, *30*(3), 685-696.

Liu, H. H., & Lee, C. M. (2019). High-capacity reversible image steganography based on pixel value ordering. EURASIP *Journal on Image and Video Processing*, 2019(1), 54.

Liu, J., Tian, Y., Han, T., Wang, J., and Luo, X. (2016). Stego key searching for LSB steganography on JPEG decompressed image. *Science China Information Sciences*, 1-15.

Liu, W., Yin, X., Lu, W., Zhang, J., Zeng, J., Shi, S., & Mao, M. (2020). Secure halftone image steganography with minimizing the distortion on pair swapping. *Signal Processing*, *167*, 107287.

Lunghi, T., Brask, J. B., Lim, C. C. W., Lavigne, Q., Bowles, J., Martin, A., ... and Brunner, N. (2015). Self-Testing Quantum Random Number Generator.*Physical review letters*, *114*(15), 150501.

Mahana, S. K., & Aggarwal, R. K. (2019, February). Image Steganography: Analysis & Evaluation of Secret Communication. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.

Maheswari, S. U., and Hemanth, D. J. (2015). Frequency domain QR code based image steganography using Fresnelet transform. *AEU-International Journal of Electronics and Communications*, *69*(2), 539-544.

Maniriho, P., & Ahmad, T. (2018). Information hiding scheme for digital images using difference expansion and modulus function. *Journal of King Saud University-Computer and Information Sciences*.

Meng, R., Zhou, Z., Cui, Q., Sun, X., & Yuan, C. (2019). A Novel Steganography Scheme Combining Coverless Information Hiding and Steganography. J*ournal of Information Hiding and Privacy Protection*, 1(1), 43-48.

Mengdi, L., Mu, K., Zhong, P., Wen, J., & Xue, Y. (2019). Generating Steganographic Image Description by Dynamic Synonym Substitution. *Signal Processing*, *164*, 193-201.

Mishra, M., Routray, A. R., & Kumar, S. (2012). High Security Image Steganography with Modified Arnold's Cat Map. *International Journal of Computer Applications*, *37*(9), 16-20.

Mohamed, M. H., and Mohamed, L. M. (2016). High Capacity Image Steganography Technique based on LSB Substitution Method. *Applied Mathematics and Information Sciences*, *10*(1), 259.

Mohapatra, C., and Pandey, M. (2015). A Review on current Methods and application of Digital image Steganography. *International Journal of Multidisciplinary Approach and Studies*, *2*(2).

Morkel, T., Eloff, J. H. P., & Olivier, M. S. An Overview Of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa. *Pretoria, South Africa*.

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*, *86*, 951-960.

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2015). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*, *86*, 951-960.

Mungmode, S., Sedamkar, R. R., and Kulkarni, N. (2016). An Enhanced Edge Adaptive Steganography Approach Using Threshold Value for Region Selection. *arXiv preprint arXiv:1601.02076*.

Nag, A., Biswas, S., Sarkar, D., and Sarkar, P. P. (2015). Semi Random Position Based Steganography for Resisting Statistical Steganalysis. *IJ Network Security*, 17(1), 57-65.

Nayak, R. (2015). Steganography with BSS-RSA-LSB technique: A new approach to Steganography. *IJSEAT*, *3*(5), 187-190.

Pal, A. K., Naik, K., & Agarwal, R. (2019). A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity. *International Arab Journal Of Information Technology*, 16(1), 116-124.

Pal, A. K., Naik, K., & Agrawal, R. (2019). A steganography scheme on JPEG compressed cover image with high embedding capacity. *Int. Arab J. Inf. Technol.*, *16*(1), 116-124.

Pandey, A., Saini, B. S., Singh, B., & Sood, N. (2019). Bernoulli's Chaotic Map-Based 2D ECG Image Steganography: A Medical Data Security Approach. In Medical Data Security for Bioengineers (pp. 208-241). IGI Global.

Parberry, I. (1997). An efficient algorithm for the Knight's tour problem.*Discrete Applied Mathematics*, *73*(3), 251-260.

Parvez, M. T., and Gutub, A. A. (2008, December). RGB intensity based variable-bits image steganography. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE* (pp. 1322-1327). IEEE.

Patel, F. R., and Cheeran, A. N. (2015). Performance Evaluation of Steganography and AES encryption based on different formats of the Image. *Performance Evaluation*, *4*(5).

Patel, K., and Ragha, L. (2015, May). Binary image Steganography in wavelet domain. In *Industrial Instrumentation and Control (ICIC), 2015 International Conference on* (pp. 1635-1640). IEEE.

Patterson, N. M., and Lee, S. F. (2015). Image Steganography.

Philip, A. (2013). A Generalized Pseudo-Knight s Tour Algorithm for Encryption of an Image. *Potentials, IEEE*, *32*(6), 10-16.

Prabhu, P., & Manjunath, K. N. (2019). Secured Image Transmission in Medical Imaging Applications—A Survey. In Computer Aided Intervention and Diagnostics in Clinical and Medical Images (pp. 125-133). Springer.

Prasad, S., & Pal, A. K. (2019). Logistic Map-Based Image Steganography Scheme Using Combined LSB and PVD for Security Enhancement. In *Emerging Technologies in Data Mining and Information Security* (pp. 203-214). Springer, Singapore.

Qu, Z., Li, Z., Xu, G., Wu, S., & Wang, X. (2019). Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm. *IEEE Access*, *7*, 50849-50857.

Rachmawanto, E. H., & Sari, C. A. (2017). Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System, 2(1), 1-11.

Rahman, M. S., Khalil, I., & Yi, X. (2020). Reversible Biosignal Steganography Approach for Authenticating Biosignals using Extended Binary Golay code. IEEE Journal of Biomedical and Health Informatics.

Raeiatibanadkooki, M., Quchani, S. R., KhalilZade, M., and Bahaadinbeigy, K. (2016). Compression and Encryption of ECG Signal Using Wavelet and Chaotically Huffman Code in Telemedicine Application. *Journal of medical systems*, *40*(3), 1-8.

Rai, P., Gurung, S., and Ghose, M. K. (2015). Analysis of Image Steganography Techniques: A Survey. *International Journal of Computer Applications*, *114*(1).

Raja, K. B., Venugopal, K. R., and Patnaik, L. M. (2006, December). High capacity lossless secure image steganography using wavelets. In *Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on* (pp. 230-235). IEEE.

Ramalingam, M., and Isa, N. A. M. (2015). A steganography approach over video images to improve security. *Indian Journal of Science and Technology*, *8*(1), 79-86.

Ramu, P., and Swaminathan, R. (2016). Imperceptibility—Robustness trade off studies for ECG steganography using Continuous Ant Colony Optimization.*Expert Systems with Applications*, *49*, 123-135.

Rani, M. M. S., Mary, G. G., and Euphrasia, K. R. (2016). Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques. In *Computational Intelligence, Cyber Security and Computational Models* (pp. 403-412). Springer Singapore.

Rao, C. S., and Devi, V. B. (2016). Comparative Analysis of HVS Based Robust Video Watermarking Scheme. In *Microelectronics, Electromagnetics and Telecommunications* (pp. 103-110). Springer India.

Rasheed, Z. A. S. (2015). ’Steganography Technique for Binary Text Image. International Journal of Science and Research (IJSR) ISSN (Online), 2319-7064.

Rayappan, J. B. B. (2013). Kubera kolam: A way for random image steganography. *Research Journal of Information Technology*, 5(3), 304-316.

Sahu, A. K., & Swain, G. (2019). An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function. *Wireless Personal Communications*, 1-16.

Saidi, M., Mannai, O., Hermassi, H., Rhouma, R., & Belghith, S. (2019). USAD: undetectable steganographic approach in DCT domain. *The Imaging Science Journal*, 1-17.

Saeed, A., Khan, M. J., Shahid, H., Naqvi, S. I., Riaz, M. A., Khan, M. S., & Amin, Y. (2020). An Accurate Texture Complexity Estimation for Quality-Enhanced and Secure Image Steganography. *IEEE Access*, *8*, 21613-21630.

Sanguinetti, B., Traverso, G., Lavoie, J., Martin, A., and Zbinden, H. (2016). Perfectly secure steganography: hiding information in the quantum noise of a photograph. *Physical Review A*, *93*(1), 012336.

Sari, C. A., Rachmawanto, E. H., & Kusuma, E. J. (2019). Good Performance Images Encryption Using Selective Bit T-Des On Inverted Lsb Steganography. Jurnal Ilmu Komputer dan Informasi, 12(1), 41-49.

Sarmah, D. K., & Kulkarni, A. J. (2018). JPEG based steganography methods using Cohort Intelligence with Cognitive Computing and modified Multi Random Start Local Search optimization algorithms. Information Sciences, 430, 378-396.

Sedighi, V., Cogranne, R., and Fridrich, J. (2016). Content-Adaptive Steganography by Minimizing Statistical Detectability. *Information Forensics and Security, IEEE Transactions on*, *11*(2), 221-234.

Seyyedi, S. A., Sadau, V., and Ivanov, N. (2016). A Secure Steganography Method Based on Integer Lifting Wavelet Transform. *International Journal of Network Security*, *18*(1), 124-132.

Shanthakumari, R., & Malliga, S. (2019). Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. Multimedia Tools and Applications, 1-17.

Shanthakumari, R., & Malliga, S. (2019). Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment. Sādhanā, 44(5), 119.

Sharma, V. K., Mathur, P., & Srivastava, D. K. (2019). Highly Secure DWT Steganography Scheme for Encrypted Data Hiding. In *Information and Communication Technology for Intelligent Systems* (pp. 665-673). Springer, Singapore.

Shelke, S. G., and Jagtap, S. K. (2015, February). Analysis of Spatial Domain Image Steganography Techniques. In *Computing Communication Control and*

*Automation (ICCUBEA), 2015 International Conference on* (pp. 665-667). IEEE.

Shyla, M. K., & Kumar, K. S. (2019). Novel Color Image Data Hiding Technique Based on DCT and Compressed Sensing Algorithm. In *Emerging Research in Electronics, Computer Science and Technology* (pp. 1151-1157). Springer, Singapore.

Silman, J. (2001). Steganography and steganalysis: an overview. *Sans Institute*, *3*, 61-76.

Singh, J., Kaur, G., and Garcha, M. K. (2015, June). Review of Spatial and Frequency Domain Steganographic Approaches. In *International Journal of Engineering Research and Technology* (Vol. 4, No. 06, June-2015). ESRSA Publications.

Singh, M., Kakkar, A., and Singh, M. (2015). Image Encryption Scheme Based on Knight's Tour Problem. *Procedia Computer Science*, *70*, 245-250.

Singh, N., & Bhardwaj, J. (2019). Comparative Analysis for Steganographic LSB Variants. In *Computing, Communication and Signal Processing* (pp. 827-835). Springer, Singapore.

Singh, S., and Datar, A. (2015). Improved Hash Based Approach for Secure Color Image Steganography using Canny Edge Detection Method. *International Journal of Computer Science and Network Security* (IJCSNS),15(7), 92.

Singh, S., Singh, R., & Siddiqui, T. J. (2016). Singular value decomposition based image steganography using integer wavelet transform. In Advances in signal processing and intelligent recognition systems (pp. 593-601). Springer, Cham.

Singh, S., Singh, R., and Siddiqui, T. J. (2016). Singular Value Decomposition Based Image Steganography Using Integer Wavelet Transform. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 593-601). Springer International Publishing.

Singh, S., Yadav, S., Raj, A., & Gupta, P. (2018, October). A Survey Paper on Different Steganography Techniques. In *Proceedings on International Conference on Emerg* (Vol. 2, pp. 103-108).

Som, S., Mitra, A., Palit, S., & Chaudhuri, B. B. (2019). A selective bitplane image encryption scheme using chaotic maps. *Multimedia Tools and Applications*, *78*(8), 10373-10400.

Song, X., Wang, S., & Niu, X. (2012, July). An integer DCT and affine transformation based image steganography method. In *2012 Eighth*

*International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 102-105). IEEE.

Srinivasan, B., Arunkumar, S., and Rajesh, K. (2015). A Novel Approach for Color Image, Steganography Using NUBASI and Randomized, Secret Sharing Algorithm. *Indian Journal of Science and Technology*, *8*(S7), 228-235.

Stanley, C. A. (2005). Pairs of Values and the Chi-squared Attack. *Master's Thesis, Department of Mathematics, Iowa State University*.

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

Swain, G. (2019). Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arabian Journal for Science and Engineering, 44(4), 2995-3004.

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.

Tao, J., Li, S., Zhang, X., & Wang, Z. (2018). Towards robust image steganography. IEEE Transactions on Circuits and Systems for Video Technology, 29(2), 594-600.

Tang, W., Li, B., Luo, W., and Huang, J. (2016). Clustering Steganographic Modification Directions for Color Components.

Thakur, P., Kushwaha, S., and Rai, Y. (2015). Enhance Steganography Techniques: A Solution for Image Security. *International Journal of Computer Applications*, *115*(3).

Thampi, S. M. (2004). Information hiding techniques: A tutorial review. *ISTE-STTP on Network Security and Cryptography, LBSCE*.

Thanikaiselvan, V., and Arulmozhivarman, P. (2013). Horse Communication against Harsh Attack: A Stego Ride. *Research Journal of Information Technology*, *5*(3), 263-276.

Thanikaiselvan, V., & Arulmozhivarman, P. (2015). RAND-STEG: an integer wavelet transform domain digital image random steganography using knight's tour. *Security and Communication Networks*, *8*(13), 2374-2382.

Tolba, M. F., Ghonemy, M. S., Taha, I. A. H., and Khalifa, A. S. (2004, July). High capacity image steganography using wavelet-based fusion. In*Computers and*

*Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on* (Vol. 1, pp. 430-435). IEEE.

Tuncer, T., and Avci, E. (2016). A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. *Displays*,*41*, 1-8.

Tutuncu, K., and Hassan, A. A. (2015). New Approach in E-mail Based Text Steganography. *International Journal of Intelligent Systems and Applications in Engineering*, *3*(2), 54-56.

Venkatachalam, S., Banu, A. S., and Padmaa, M. (2015). A Robust Image Steganography using CDF Lifting Scheme and Huffman Encoding.*International Journal of Computer Applications*, *110*(11).

Venugopal, D., Mohan, S., and Raja, S. (2016). An efficient block based lossless compression of medical images. *Optik-International Journal for Light and Electron Optics*, *127*(2), 754-758.

Vikranth, B. M., Momin, M. H., Mohsin, S. M., Rimal, S., and Pandey, S. R. (2015, April). A Survey Of Image Steganography. In *Journal of Emerging Technologies and Innovative Research* (Vol. 2, No. 4 (April-2015)). JETIR.

Wang, J., Cheng, M., Wu, P., & Chen, B. (2019). A Survey on Digital Image Steganography. *Journal of Information Hiding and Privacy Protection*, *1*(2), 87.

Wang, X., Wei, C., and Han, X. (2015). Steganography forensics method for detecting least significant bit replacement attack. *Journal of Electronic Imaging*, *24*(1), 013016-013016.

Weng, S., and Pan, J. S. (2016). Integer transform based reversible watermarking incorporating block selection. *Journal of Visual Communication and Image Representation*, *35*, 25-35.

Westfeld, A. (2002, October). Detecting low embedding rates. In *International Workshop on Information Hiding* (pp. 324-339). Springer, Berlin, Heidelberg.

Wu, A., Nowak, M. J., Wicks, M., & Zhang, Z. (2016). Bio-inspired RF steganography via linear chirp radar signals. *IEEE Communications Magazine*, *54*(6), 82-86.

Wu, B., Chang, M. P., Shastri, B. J., Ma, P. Y., & Prucnal, P. R. (2015). Dispersion deployment and compensation for optical steganography based on noise. *IEEE Photonics Technology Letters*, *28*(4), 421-424.

Wu, M. Y., Ho, Y. K., & Lee, J. H. (2004). An iterative method of palette-based image steganography. *Pattern Recognition Letters*, *25*(3), 301-309.

Xue, Y., Liu, W., Lu, W., Yeung, Y., Liu, X., & Liu, H. (2019). Efficient halftone image steganography based on dispersion degree optimization. *Journal of Real-Time Image Processing*, *16*(3), 601-609.

Yahya, A. (2019). Characteristic Region-Based Image Steganography. In *Steganography Techniques for Digital Images* (pp. 43-83). Springer, Cham.

Yahya, A. (2019). *Steganography Techniques for Digital Images*. Springer.

Yan, F., Iliyasu, A. M., and Venegas-Andraca, S. E. (2016). A survey of quantum image representations. *Quantum Information Processing*, *15*(1), 1-35.

Yang, B., Rozic, V., Mentens, N., and Verbauwhede, I. (2015). On-the-Fly Tests for Non-Ideal True Random Number Generators. In *IEEE International Symposium on Circuits and Systems (ISCAS 2015)*.

Yang, C. H., Lin, Y. K., Chang, C. H., and Chen, J. Y. (2016). Data Hiding for H. 264/AVC Based on the Motion Vector of 16 Grids. In *Advanced Multimedia and Ubiquitous Engineering* (pp. 389-395). Springer Berlin Heidelberg.

Yeung, Y., Lu, W., Xue, Y., Chen, J., & Li, R. (2019). Secure binary image steganography based on LTP distortion minimization. *Multimedia Tools and Applications*, 1-22.

Yeung, Y., Lu, W., Xue, Y., Huang, J., & Shi, Y. Q. (2019). Secure binary image steganography with distortion measurement based on prediction. IEEE Transactions on Circuits and Systems for Video Technology, 30(5), 1423-1434.

Yi, X., Yang, K., Zhao, X., Wang, Y., & Yu, H. (2019). AHCM: Adaptive Huffman Code Mapping for Audio Steganography Based on Psychoacoustic Model. IEEE Transactions on Information Forensics and Security, 14(8), 2217-2231.

Yiannakou, M., Trimikliniotis, M., Yiallouras, C., and Damianou, C. (2016). Evaluation of focused ultrasound algorithms: Issues for reducing pre-focal heating and treatment time. *Ultrasonics*, *65*, 145-153.

Younus, Z. S., & Hussain, M. K. (2019). Image steganography using exploiting modification direction for compressed encrypted data. *Journal of King Saud University-Computer and Information Sciences*, Apr, 13.

Zanganeh, O., and Ibrahim, S. (2011). Adaptive image steganography based on optimal embedding and robust against chi-square attack. *Information Technology Journal*, *10*(7), 1285-1294.

Zargar, A. J., and Singh, A. K. (2016). Robust and imperceptible image watermarking in DWT-BTC domain. *International Journal of Electronic Security and Digital Forensics*, *8*(1), 53-62.

Zhang, H., Wei, X., Wang, R., & Meng, F. (2019). An Efficient Base Conversion Using Variable Length Segmentation and Remainder Transfer. *IEEE Signal Processing Letters*, *26*(8), 1227-1231.

Zhang, J., Lu, W., Yin, X., Liu, W., & Yeung, Y. (2019). Binary image steganography based on joint distortion measurement. Journal of Visual Communication and Image Representation, 58, 600-605.

Zhang, R., Dong, S., & Liu, J. (2019). Invisible steganography via generative adversarial networks. *Multimedia Tools and Applications*, *78*(7), 8559-8575.

Zhang, W., Wang, S., and Zhang, X. (2007). Improving embedding efficiency of covering codes for applications in steganography. *Communications Letters, IEEE*, *11*(8), 680-682.

Zhang, X., and Wang, S. (2005). Steganography using multiple-base notational system and human vision sensitivity. *Signal Processing Letters, IEEE*,*12*(1), 67-70.

Zhelezov, S. (2016). Modified Algorithm for Steganalysis. *Mathematical and Software Engineering*, *1*(2), 31-36.

# LIST OF PUBLICATIONS

## Online Journal Paper


Mahdi Hashim, M.O.H.A.M.M.E.D., Rahim, M. and Shafry, M., 2017. IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION. *Journal of Theoretical & Applied Information Technology*, *95*(22). (Scopus).

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. (Scopus).

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. (Scopus).

Hashim, M., MOHD RAHIM, M. S., & ALWAN, A. A. (2018). A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. *Journal of Theoretical & Applied Information Technology*, *96*(4). (Scopus).

Domain, W.T.I.S., 2018. A review and open issues of diverse text watermarking techniques in spatial domain. *Journal of Theoretical and Applied Information Technology*, *96*(17). (Scopus).

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. (Scopus).

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. (Scopus).

Taha, Mustafa Sabah, Mohd Shafry Mohd Rahim, Mohammed Mahdi Hashim, and Hiyam N. Khalid., 2020. Information Hiding: A Tools for Securing Biometric Information. (Scopus).

Mustafa, S. T., Mohd Shafry Mohd Rahim, Falah YH Ahmed, and Mohammed Mahdi, 2020. Hiding Financial Data In Bank Card Image Using Contrast Level Value And Text Encryption For Worthiness A Robust Steganography Method. (Scopus).

**Online Scopus Conference Paper**

Taha, M.S., Rahim, M.S.M., Lafta, S.A., Hashim, M.M. and 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. (Scopus Conference).

Mahdi, M.H., Abdulrazzaq, A.A., Rahim, M.S.M., Taha, M.S., Khalid, H.N. and 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. (Scopus Conference).

Hashim, M.M., Mohsin, A.K. and Rahim, M.S.M., 2019, September. All-encompassing Review of Biometric Information Protection in Fingerprints Based Steganography. In *Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control* (pp. 1-8). (Scopus Conference)

Hashim, M.M., Taha, M.S., Aman, A.H.M., Hashim, A.H.A., Rahim, M.S.M. and 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. (Scopus Conference).

Hashim, M.M., Taha, M.S.,Rahim, M.S.M. Based on IoT Healthcare Application

for Medical Data Authentication: Towards A New Secure Framework Using Steganography . In *IOP Conference Series: Materials Science and Engineering*. IOP Publishing. (Scopus Conference).

**Accepted Papers and Conference**

Mohammed Mahdi Hashim, Mohd Shafry Mohd Rahim, Mustafa Sabah Taha. Concealing Critical Data in Medical Image by emphasized Triple decomposition for worthiness a novel steganography method. Multimedia Tools and Applications -Springer 2020 (clarivate Q2).

Mohammed Mahdi HASHIM, Mustafa Sabah Taha, Mohd Shafry Mohd Rahim. Based on Pseudo White Space and Chaotic Logistic Map: A Robust Software Watermarking Tool for Software Program. Walailak Journal of Science and Technology (WJST) (Scopus)