ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DIGITAL IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN A COMPREHENSIVE REVIEW

[1]MOHAMMED SABRI ABUALI, [2]C.B.M. RASHIDI, [3]MUATAZ H. SALIH, [4]R. A. A. RAOF, [5]SAFA SAAD HUSSEIN

[1] School of Computer and Communication Engineering,
Kangar, Perlis, Malaysia
[2]Senior Member IEEE. Advanced Communication Engineering,
Centre of Excellence, School of Computer and Communication Engineering,
Kangar, Perlis, Malaysia
[3]Senior Member IEEE. FLex, Penang, Malaysia
[4]School of Computer and Communication Engineering,
Kangar, Perlis, Malaysia
[5]School of Computer and Communication Engineering,
Kangar, Perlis, Malaysia
E-mail: [1]mohmedsabry847@gmail.com, [2]rashidibeson@unimap.edu.my, [3]muataz.aldoori@flex.com
[4]rafikha@unimap.edu.my, [5]Eng.safa86@yahoo.com

ABSTRACT

Prevalent current day scenario with the predominant accelerated utilisation of the internet, is witnessing the increased interest in the method of transmitting concealed secret information (information hiding) via several variant techniques. One of the eminent and significant form of information hiding is Steganography. Hence, Steganography involves scientific techniques in concealing information inside the host object, which serves as the transporter of the hidden information, to be communicated in a secured undetected and safe form to another party. It engages multitudinous forms of host carriers that could be utilised in the form of texts, audio, visual images, protocols and DNA. Due to its frequent use on the internet, digital images are the favoured form of carrier host documents.. This study reviews the various latest related publications pertaining to image Steganography within the spatial domain, by assessing, accumulating, synthesising and analysing the difficulties, problems and issues faced in these different studies.. The objectives of this study is to execute a review as to render a summary of image Steganography, and to compare certain elements between the selected studies. Discussions will be made in accordance to the selection of pixel for the images, the capacity of the payload and the embedding algorithm, which will enable significant research issues for future researches. It is also aimed in the furtherance of securing a more robust Steganography technique.

Keywords: *Information Hiding , Image Steganography , Spatial Domain , Stego-Image , Different Types Of Steganography.*

1. INTRODUCTION

As the result of recent development in the accrual utilisation of the internet for digital communication purposes, there has been a significant rise in research endeavours in the development of hiding information. Due to the increased risks in terms of security and privacy of information being transferred, of data or information being intercepted, accessed or maliciously modified, information hiding mechanisms has become one of the solutions in overcoming these ominous threats. Thus, Information Security is a process of acquiring more secured information, without its integrity and privacy being compromised.

As the result of this requirement, two types of information hiding techniques have been developed for data and information protection, namely; Steganography and Watermarking. They are both associated with a common construct [1][2]. In the first instance, Steganography qualifies the provision of a robust, high security mechanism. It is an intelligent method of hiding concealed data within a hosting media which acts as a carrier to defend it from intrusive unauthorised accessed or intrusion. It acts in a stealth mode, undetected, and is mediated through a host object or media as the carrier of concealed embedded secret information.

Steganalysis is the detection and deciphering of hidden secret data via the analysis of the stego media [3][4]. In the second instance, Watermarking is a mechanism in concealing secret data within the host or carrier media for the provision of the confidentiality and integrity of the information. It is utilised to verify component credibility, or to ensure recognition of digital ownership in terms of Intellectual Property or copyright issues. Digital watermark remains intact and could not be compromised through any means such as manipulation, compression and decompression. A pair of watermarking are known as; (1) visible watermarking and (2) invisible watermarking. Digital watermarking is differentiated from Steganography in terms of its objectives. Digital watermarking is aimed at ensuring copyright protection against abuse and infringement, used for source tracking and others. Table (1) explains the difference between digital steganography and digital watermarking [5][6]. There are various media carriers or host objects comprising DNA, audio, video, text and image that can be utilised with Steganography technique, which will be explicated later. Steganography when incorporated with the use of the various types of digital image formats, is a robust and secure form of covert transmitter. Image Steganography is a system that hides messages, data or information secretly within a carrier image. It is an alternative mode of mechanism in relaying information through stealth means, covertly and secretly when encryption is not possible to be used to maintain the confidentiality and security of the secret message.

-Steganography that utilises mechanisms which embed secret messages in images is classified into spatial domain and transform domain. It should be noted that the latest papers on the subject matter of Image Steganography demonstrates that 'Spatial Domain' is significant across many applications. Thus pertinent and appropriate literatures were chosen in this study, whereby the focus were drawn towards the analysis of the essential characteristics and the challenges faced by the utilisation of Image Steganography techniques.

Steganography applications are utilised in many fields and industries such as online transactions, military, medical, smart ID, communications and many others as will be explained later [7][8].

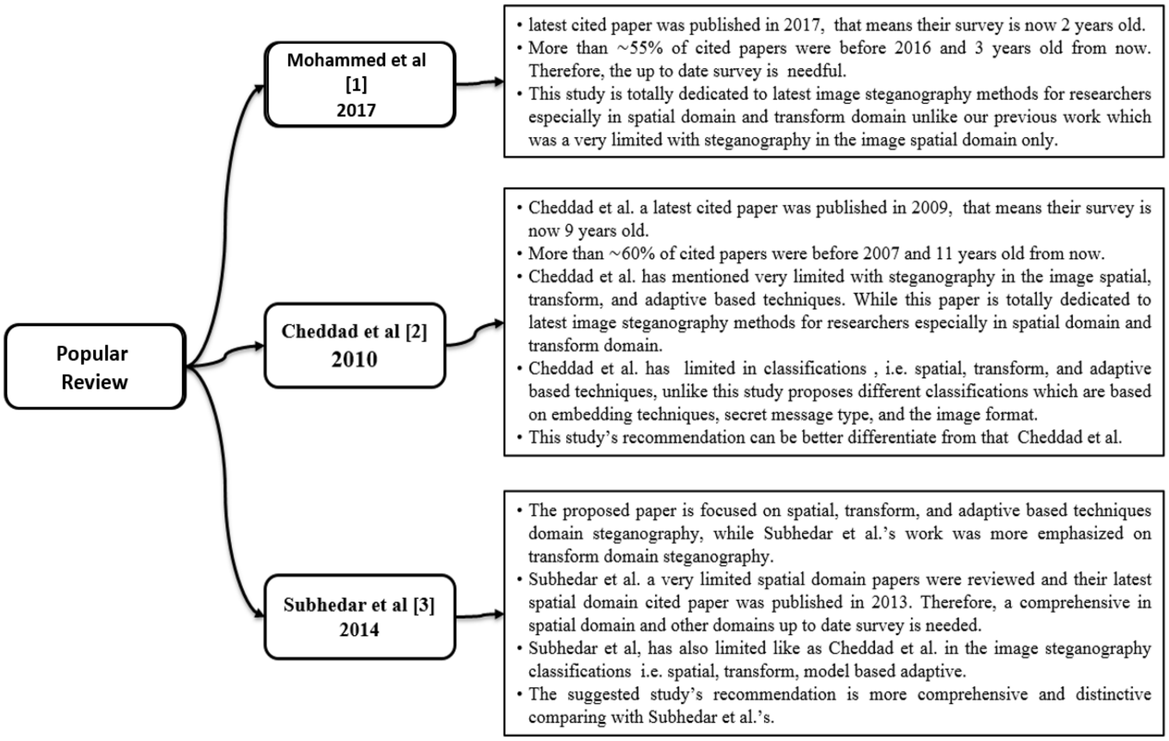
There has been a number of published reviews on Steganography, with the most significant review published in 2018 [9]. The said review emphasises on fundamental concepts, various evaluation measures, Image Steganography system security issues which includes prior literature and publications pertaining Steganography up to the publication date of the said review paper.

Table 1: Difference Between Digital Steganography And Digital Watermarking

Characteristics	**Steganography**	**Watermarking**
Cover selection	Free cover selection	Restriction
Target	maintain the confidentiality data from the detection	Maintain the authenticity of the cover object
Challenges	Security ,Imperceptibility and Capacity	Robustness
Key Requirements	Optional	Optional
Output	Stego-file	Watermarked-file
Attack	Steganalysis	image processing systems
System validity	If the secret data is detected	If the secret data is Removed or replaced
Visibility	invisible	Visible / Invisible
Robustness	against detection of hiding secret information	Against manipulate or delete secret information

However, it should be noted that this said review and other past reviews might be outdated or there has been new discoveries or contributions to this particular field of Steganography. Thus, it is necessary that we set out on our pertinent and succinct new review in this study, to add on to the pool of knowledge. We set out to review and summarise relevant past studies and surveys on Image Steganography, domains and techniques, without going into much details and discussions on the huge amount of contributions in this area [10][11]. What sets our current study apart from the rest is that it summarises prevalent techniques in Spatial Domain, in addition to analysing the variant challenges and the various obstacles of individual techniques that were created for the past number of years. Choice of pixel, embedding algorithm and capacity are the basic items that are being gauged in this current study by comparing other studies. The selection of pixel utilised is to obtain security objectives for example the sorting technique [12], Adaptive Image Segmentation (AIS)[13] and Randomised Secret Sharing (RSS) [14].

Meanwhile, the second criteria defines the ultimate number of covert information which can possibly undergo an embedding procedure within the cover image with no possibility of resulting in image quality retraction. Imperceptibility, that is the original image quality which is kept intact and as similar as possible, is obtained through the utilisation of embedding algorithm. This is enabled by preserving the pixel value resembling the original value as far as possible.It should be noted that this current study will explicate thoroughly the spatial domain techniques which however is not inclusive of transform domain. The fundamental contribution of this study is to scrutinise the variant techniques in spatial domain, to distinguish and establish the problems that are present, and to expose relevant thought-provoking research issues in this field of study.The ensuing writings in this paper are arranged according to the following parts of eight; Part 2 comprises an Overview of Steganography, Part 3 is on Various Kinds of Steganography and Part 4 is on Protocols of Steganography. Furthermore, Part 5 explains the Properties of Steganography, Part 6 is on the Application of Steganography, Part 7 explicates the Embedding Methods in detail, Part 8 explains the future trend and its proposed solution ,and finally, Part 9 is the Conclusion.



- latest cited paper was published in 2017, that means their survey is now 2 years old.
- More than ~55% of cited papers were before 2016 and 3 years old from now. Therefore, the up to date survey is needful.
- This study is totally dedicated to latest image steganography methods for researchers especially in spatial domain and transform domain unlike our previous work which was a very limited with steganography in the image spatial domain only.

- Cheddad et al. a latest cited paper was published in 2009, that means their survey is now 9 years old.
- More than ~60% of cited papers were before 2007 and 11 years old from now.
- Cheddad et al. has mentioned very limited with steganography in the image spatial, transform, and adaptive based techniques. While this paper is totally dedicated to latest image steganography methods for researchers especially in spatial domain and transform domain.
- Cheddad et al. has limited in classifications , i.e. spatial, transform, and adaptive based techniques, unlike this study proposes different classifications which are based on embedding techniques, secret message type, and the image format.
- This study's recommendation can be better differentiate from that Cheddad et al.

- The proposed paper is focused on spatial, transform, and adaptive based techniques domain steganography, while Subhedar et al.'s work was more emphasized on transform domain steganography.
- Subhedar et al. a very limited spatial domain papers were reviewed and their latest spatial domain cited paper was published in 2013. Therefore, a comprehensive in spatial domain and other domains up to date survey is needed.
- Subhedar et al, has also limited like as Cheddad et al. in the image steganography classifications i.e. spatial, transform, model based adaptive.
- The suggested study's recommendation is more comprehensive and distinctive comparing with Subhedar et al.'s.

Figure 1. The Main Criteria Of Different Review Papers

Several review on steganography have been published within recent years, the most important and popular are three papers published in recent years ago [1][47][9]. these papers are focusing on a review of essential concepts, variety of evaluation measures, security side of image steganography system and includes the literature that have been published until the time the papers was published. Nevertheless, this review may be considered out of date due there are many of contributions published from that date, these new publications necessarily to be collect within a new review paper.

Briefly discussed some other surveys the image steganography's definition, domains as well as techniques in a summarized form without discussing the huge amount of contributions on this area, with respect to the review papers.

While the difference in our work summarizes the current image steganography techniques in spatial domain and adaptive domain also analyzed different problems and the drawbacks of each method that have been innovated from last few years. Figure1 explain the main difference between these review papers according to different criteria. Our work comes to complete these criteria with a recent Studies on steganography in both spatial and adaptive domain.

2. STEGANOGRAPHY:ANONVERVIEW

The etymology of Steganography originates from a pair of Greek lexical items, Steganos and Graphy, which denotes "covered" (i.e. secret) and "writing" respectively[15].Initial orthographic proof pertaining to Steganography can be traced back circa 440BC, from the affirmation of Herodotus, who was a Greek historian [16]. Various means of hiding information had been carried out in the past. The Ancient Greek had missive written on wooden tablets which they coated with wax to conceal the messages. In addition to this, they had tattooed messages on the shaven heads of messengers, and await for the regrowth of their hair to cover and hide the messages before these messengers were sent out as carriers of secret messages [17]. Meanwhile, during the Second World War, the Germans had invented the microdot technology in several stages, and had utilised cover materials such as magazines so as not to arouse suspicions [18].

During World War II, messages were written with invisible ink between the lines of normal looking letters that would not attract attention. Messages were open coded by the German spies during World War II, as the messages seem innocent and inconspicuous, hidden in the carrier note [17]. There is an extensive pool of subject-specific literature on the matter for those who are interested in further elaboration [17][19][20] The developments in Steganography have enabled the creation of variant and astute techniques of secret messages to be embedded within varying digital media such a text media, video, protocol, DNA and audio, with the current accessibility of the internet and dynamic computers.

Conventionally, the mechanism of hiding information by embedding them in a discrete way; termed as Steganography, entails the existence of the concealed data is a mutual knowledge only shared between the specific and exact interlocutors as illustrated in figure2.The hidden information is the stego object file. It is then relayed to the receiver, where the concealed information is retrieved and deciphered by the receiver through the application of extracting algorithm [21]. The general Steganography mechanism is depicted in figure 2.

There are four principal constituents in the fundamental Steganography model:

1- Media carrier: The image that is used to conceal the image is known as the cover image or the cover object, will act as the host to transmit the covert information concealed within it.

2- Secret data: A covert information may comprise of data, file or image and others.

3- Secret Key: A covert key which is termed as the Secret Key is utilised to encode /decode in the deciphering of the concealed information.

4- Stego media (Y): The Stego media is also known as the stego object. This stage is reached ensuing the process of embedding the covert information.

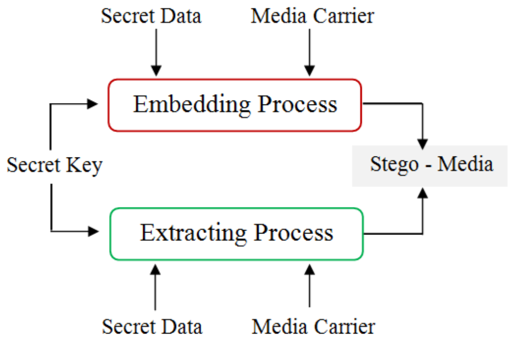


Figure 2. A general block diagram of Steganography Process.

3. TYPES OF STEGANOGRAPHY

Digital images are the favoured form of all digital media in Steganography due to their regularity of being used and availability on the internet, although all other digital file formats are also utilised[22]. Figure 3 illustrates six primary categories formats of files that can be utilised for Steganography

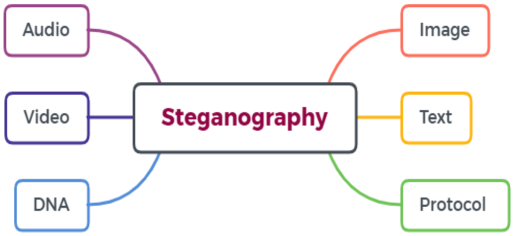


Figure 3 : Types of Steganography

i. *Image Steganography.* The most popular form of cover objects that is frequently utilised for Steganography are digital images, as they are also the most dominant forms found on the internet. A covert information is embedded within the digital image at the time of an algorithm with the assistance of a secret key which produces a stego image. This method mainly involves the intensities of pixels utilised to conceal the covert information [23] [24].

ii. *Video Steganography*. Concealing covert information in the form of video format is termed as Video Steganography. Video files comprise of a compilation of images and audio. Typically, an extensive number of the recommended techniques on images and audio can be applied to video files as well. It is the most suitable form of image file when compared to the other multimedia files. This is due to the capacity of space inside the video format that can accommodate and conceal huge amount of data, which can go undetected by people as the result of the endless stream of information. Various kinds of video files that can be utilised are H.264, Mp4, MPEG, AVI or other video formats [25][26].

iii. *Text Steganography*. Concealing (hiding) covert information within a text file is termed as text Steganography. It possesses minuscule memory size, thus it is only able to be repository for text format only. There are numerous formats utilised using this mechanism. The tabs, capital letters and number of white spaces are utilised to hide information in Text Steganography. It is rarely utilised as text files retain a huge amount of surplus redundant data [27][28].

iv. *Protocol Steganography*.This technique involves the embedding of the covert information inside the network protocols, for example IP, TCP, ICMP, UDP and others; whereby the protocol is utilised as a carrier. The composition of a network packet comprises the user data, packet headers and packet trailers. Thus, Steganography can be utilised within the network model layers. This terminology is identified as Protocol Steganography [29] [30]

v. Audio Steganography . Digital sound which has undergone covert information embedding is known as Audio Steganography which utilises computer as the basis for its system to function. The minor modification made to the sequential arrangement of the binary in a sound system enables the embedding of covert information in it.Certain software for audio steganography that is currently available is an information embedding enabler, that allows information to be concealed in WAV, AU, and MP3 sound files [31]. The task of embedding covert information in digital sound is more daunting as compared to the same task to be executed in other media forms such images in digital forms. Various techniques in the embedment of data in digital audio were injected and initiated into the audio environment to culminate in a running system that will hide covert information well. These variant techniques run on a spectrum that consists of the introduction of data via signal noise form through the utilisation of uncomplicated algorithm, right up to stronger techniques such as the employment of higher technology mechanisms to conceal data [32].

vi. DNA Steganography. In DNA-based Steganography, the distinctive chaotic character of DNA enables the assigning of covert information to be embedded. Lately, there is a method that has been employed which utilises the numerical mapping table to superimpose and match the DNA sequence for enciphering covert data [33][34] .

4. PROTOCOLS OF STEGANOGRAPHY

Predominantly, there are three kinds of protocols: (i) Pure Steganography, (ii) Secret Key

Steganography and (iii) Public Key Steganography[35].

i. ***Pure Steganography :*** It involves a system whereby the interlocutors who are sending and receiving the secret messages do not share prior information [18]. In the said case, it is imperative that both The sender and receiver possess the access to embedding and retrieving functions which should not be a common knowledge to a third party. In reality, Pure Steganography is not protected due to the fact that it is conflicting with Kerckhoff's principle which is grounded on the premise that the embedding algorithm is known to The third party [36].

ii. ***Secret Key Steganography :*** With reference to Kerckhoff's principle, it is inferred that the third party possesses a channel towards the extraction method, and hence this enables him /her to intercept and retrieve the covert information that is hidden in every stego media transacted between The sender and receiver . Hence, the shared knowledge of the stego-key by the sender and receiver has impact upon the security of the hidden information. The absence of this key will result in total hindrance for any party to access the secret information from the cover stego media [36]. Nevertheless, the added relaying of the secret key is conflicting with the primary objectives of Steganography; that is imperceptible communications, presuming the case that The sender and receiver had a shared knowledge of the stego key previously .

iii. ***Public Key Steganography:*** It utilises a pair of keys; the public key and the private key. The public key is deposited into a public database and is utilised by embedding algorithm, meanwhile the private key is utilised by the extraction algorithm to retrieve the secret message.Hence, the public key is able to be constructed by the utilisation of public cryptosystem, where The sender and receiver need not interchange the secret key. This can be carried out on the premise that it is presumed that the sender and receiver have shared their public key with each other prior their detention [18]. On the hypothesis that The third party has knowledge pertaining the embedding method, she may attempt to retrieve the hidden information within the stego media. Nonetheless, she will fail in identifying the secret information due to the fact that they will appear as chaotic strands of bits as an encryption result.

5. PROPERTIES OF STEGANOGRAPHY

Steganography is associated with a more extensive field termed as information hiding, thus the overall characteristics of information hiding can be applied for both Steganography and Digital Watermarking. However, Steganography is to some degree unlike Watermarking in terms of prioritisation and definitions of these properties as explicated herewith:

i. ***Undetectability:*** The essential objectives of Steganography is to hide information that will conceal the presence of the secret information and keep it discreet. Hence, undetectability is the utmost paramount property of all Steganography system, denoting that the presence of any covert information should go undetected by the utilisation of any statistical methods. In the event that any person is able to readily detect and identify the stego media, it could be surmised that the utilisation of the specific Steganographic technique is senseless [15]. There are several factors that could directly impact on the undetectability, such as the cover media chosen, the embedding technique and the amount of modifications imposed on the cover media [37]. Nonetheless, there is a non-existent method by any Steganographic technique which are able to embed information within certain media file that will not leave residual artefacts. Thus, the lesser possibility of distinguishing these artefacts implicates a more superior Steganography technique over others. These are the reasons why it is not sufficient to just being able to create a new Steganographic technique when it is not able to attribute a reduced probability of detection by the utilisation of present day techniques.

ii. ***Imperceptibility :*** Imperceptibility is one of the properties of Steganographic system, which defines the compulsion of stego media to be free of any residual detectable artifacts ensuing the embedding of the secret data [38]. Thus, in their embedding operation, a majority of the Steganographic techniques accounted on the restrictions of the Human Visual System (HVS) or Human Auditory System (HAS) [39]. This implicates that, as an exemplar, the stego image should appear as a harmless and innocent image by HVS. There are a multitudinous number of evaluation criteria with respect to imperceptibility, which should be taken into account in terms of the kind of Steganography technique, or cover file kind utilised for concealing the data (data hiding).As an exemplar, the size of the file could indicate the existence of a concealed data in the text files or the insertion-based Steganography. In addition to that, in the case of Image Steganography, the quality of the image could indicate the presence of a substitution-based Image Steganography. However, prevalent Steganographic techniques escape detection and have a robust level of imperceptibility, however, are handicapped by identification through statistical means.

iii. ***Security :*** In Steganography literature, the terminology 'security' is equated to 'undetectability'. Hence, statistical undetectability ensures the security of a Steganographic technique [40].
Nonetheless, it should be noted that a majority of prevalent Steganographic techniques are taking into account of the passive attack, however the consideration on active attacks are taken into consideration at a much lesser degree in literature as debated by [41].

iv. ***Capacity :*** The embedding capacity and the Steganographic capacity are the two variant types of capacity associated with the field of Steganography [40]. Embedding capacity is the ultimate quantity of bits that a specific media file is able to accept to be embedded. As an exemplar, a grayscale image capacity to be embedded with LSB replacement is equivalent to the total amount of image pixels, which denotes the embedding capacity. However, Steganographic Capacity is unlike embedding capacity as it is difficult to ascertain the capacity even in an uncomplicated embedding technique. It is denoted by the optimum amount of bits that is able to be embedded in a specific media file with inconspicuous presence that could not be detected by an attacker.

v. ***Robustness :*** Robustness in Steganography is impacted by two factors. Firstly, in terms of undetectability as explicated in the previous section.Secondly is the capability to overcome active attack, which is more significant in digital watermarking [42]. This signifies that the enablement of the secret information to be retrievable by another entity, equally so in circumstances of the cover media having undergone through certain extent of data processing [15]. The robustness of a Steganographic Technique is accounted by its strength to be able to withstand both detection and destruction of the the hidden information, making both tasks arduous for the attacker to uncover. However as asserted by [40], overcoming active attack is not the main concern of Steganography as it is scarcely ever been considered in the equation. This is brought about by the premise of assumption that the stego object will be transmitted via the network. Hence it is also assumed that degradation is negligible, and that the receiving second party would receive the message by the first party intact.

6. APPLICATION OF STEGANOGRAPHY

The utilisation of a secure and stealth mode of communications is practised in a majority of fields. Those who benefit from this modus operandi mode of communication are those involved in the military, medical, multi-media and various industries where security issues are of great importance, and that a covert channel of communication is imperative for the utilisation within and outside. For example in the medicinal area where confidentiality of medical data is of high priority, important information are concealed within the data itself, with sequence DNA, and are propagated safely and securely. This will assist in the circumvention of private data leakage into unauthorised hands. Reversible Steganography systems are the norm as the cover and covert information must be retrieved singly for the recipients end. The nature of securedness and protection is of utmost essence and priority in the army and security communications. Free and accessible conduits may be intercepted, in addition to being compromised, thus authorised mode of communications is imperative. In this instance, the application of a multi-layered encryption method is implemented to the Steganographic systems prior the embedding process.

Its frequent execution in multi-media applications is to mark copyright matters. Hence watermarking entails this application type, whereby the cover media is of greater eminence than the covert information. Additionally, within the world of corporate communications, in addition to a majority of industries, authenticity and security overrides other factors and is deemed more significant, as not secured communications, with a probability of severe information exposure. Certain methods of applying it are discussed in this study which include Smartsteg through mobile gadgets [43], Steganography was used in telemedicine (WBAN)[44], IP (Intellectual Properties) protection and the embedment of unique data within smart identification card [45]. Amongst the advanced Steganography techniques known is its utilisation of a sophisticated data framework; in assisting the facilitation in securing an expansive data. Meta information is utilised with it in end-to-end data transmission of the actual data which is transmitted in a secure manner. Big data problems are resolved by the utilisation of up-to-date information construct, to resolve the allocation issues within the hard-disc memory[46]. Fujitsu is the renown Japanese company which was responsible for the invention of an encryption system that encrypts information into an image format which is then ensued in its print version , imperceptible and concealed away from vision detection, but could be decrypted through a hand-held camera.

The entire decryption mechanisms is undertaken in micro-seconds due to the magnitude of covert data is just 12 bytes [47]. The rational behind the popular demand for Steganography is due to its ethical utilisations as well as unethical utilisations by cyber-criminals who embed viruses, spamwares and malwares to the information.

Thus, an accelerated development in the last ten years has served as a magnet to the mass throughout various domains. Heightened by the fact of the ease of availability of Steganography tools online which avail the layperson without any technical know-how to explore and engage in unethical cyber-crime activities. An example of such a tool is Xiao Steganography which allows the individual who uses it to disclose a firm's confidential data in mere triple measures, with the ensuing steps executed by the tool [48]. The measures entail choosing a host image, embed whatsoever covert message written, on the other hand choose a covert file, which is ensued by pushing the Button for embedding.

Since the image format is a common data denominator that runs across the board of all applications in the current digital communications era, Image Steganography has an essential role to play. Thus, due to the great influx of images, detecting secret data amongst the millions of images is a daunting task and is almost impossible in the event of it being transmitted securely.

7. STEGANOGRAPHY IN DIGITAL IMAGE

There have been a plethora of secret communication methods created and improved upon over the past several ten years, whereby Image Steganography constitutes amongst the main fields of stealth communication [49][50][38][20][42]. This is due to the fact that there are millions of ready and available images on the internet of which any individual who wishes to communicate in a secret way, may embed their own messages in them [51]. Furthermore, there is a high capacity of redundancy in the format, and minute modifications to the digital images are undetected by HVS. Moreover, their presence are everywhere (Omnipresent) on the internet, thus they are readily utilised as cover media to embed data without arousing [52][53] Hence, digital images are rampantly utilised as cover media for Steganography. Relatively a majority of the Steganographic systems explore and utilised the knowledge of Human Visual System in the embedding techniques [52] [54] [55] Thus, regions that are noisy and on the edges of images attracts the interest of Steganographers, as the HVS is less susceptible to the noisy regions and areas on the edges [56].

Despite certain progress that has been made on Image Steganography in terms of Binary Images,[57- 59] and 3-D images, researchers focus their study on concealing data in grayscale and colour images. Even though the luminance component of colour image is identical to that of grayscale image, a few experts regard grayscale images as the optimum cover for Steganography [60,61]This is due to the fact that the process of embedding will modify the correlation between the colour elements, and these changes can cause artefact traces which heightened the ease of embedding detection.

Typically, there are two main types of Image Steganography; the Spatial Domain and the Transform Domain.Figure 4 illustrates the two types of methods. This section will explicate the Spatial Domain in detail, meanwhile the Transform Domain and adaptive Domain which is a special form of Spatial and Transforms techniques will be explained concisely.Table (2) explains the dissimilarity between them

i. *Transform Domain Image Steganography .*

The values that are related to the Transform Domain are utilised in the insertion and combination of covert bits within an image found in cover image. The secret bits are concealed under the sub-band frequency coefficients during the utilisation of the Transform Domain based techniques. Transform Domain techniques involves a more complex process of embedding and decoding as compared to the time domain techniques. The system securedness will hence be enhanced. Another advantage of the Transform Domain Technique is that it is less susceptible to rotation attacks, cropping, compression, scaling, hence enabling systems that are founded on Transform to be of greater efficiency. Transform Domain techniques are widely utilised in the field of Steganography, and the preferred scheme choices consist of Integer Wavelet Transform (IWT), Complex Wavelet Transforms (CWT), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and different versions of these basic transforms and Dual-Tree Complex wavelet transforms (DTCWT),

Manuscripts must be in English (all figures and text) and prepared on Letter size paper (8.5 X 11 inches) in two column-format with 1.3 margins from top and .6 from bottom, and 1.25cm from left and right, leaving a gutter width of 0.2 between columns.

ii. ***Adaptive* Steganography.**

This is a specific form of Spatial and Transform techniques. In addition, it is termed as “Model-Based”[62] or“Statistics-aware embedding”or “Masking”[63]. A huge portion of core work pertaining Steganography can be categorised under this section.The introduction of the adaptive nature within the embedding scheme can be executed in a various ways such as the selection of target pixels within the cover image, the type of modification to be implemented, the amount of bits embedded in a pixel and many others. The classification of systems can be divided into several sections, and are founded on the attributes and the provisions of adaptive methods through the systems. These encompass Region Based Steganography, Human Visual System (HVS) based Steganography, Machine Learning and Artificial Intelligence Techniques based Steganography [9] .

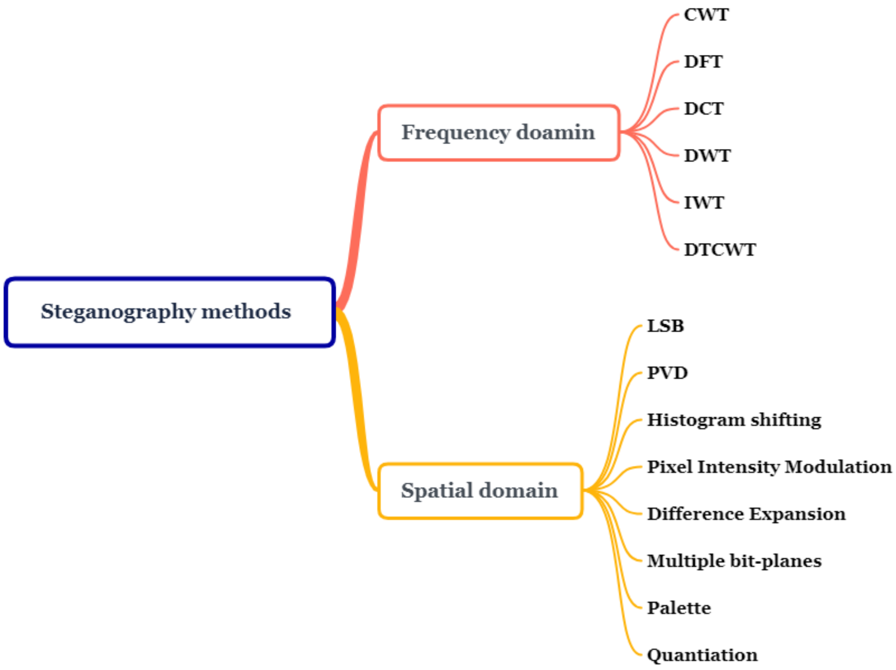


Figure 4 : Types of Steganography methods

Albeit these factors, various alternative kinds of Image Steganography are seldom used or lesser known. One such exemplar is affixing the secret information to the end of file (EOF) tag of a JPG image which is uncomplicated, and in most instances will be overlooked by image viewer applications. The said data embedment type is effortless, has no alteration impact on the quality of the image, makes no modification to the image histogram, and cannot be perceived by image viewer applications. Nonetheless, in circumstances that the stego image is accessed via other applications such as the Notepad, covert data will be displayed, due to the fact that the configuration of the Notepad is not configured to address EOF tag of the JPG file. Other exemplar is the concealed information that has been affixed to the image's extended file information (EXIF), which is the common day practice and utilised by digital cameras manufacturers as a repository of information such a camera's make and model, the photo capturing time, its resolution and other information. As asserted by [64] , the information collected and displayed by the EXIF could assist in picture authenticity and verification in an investigative procedure associated with child pornography. The utmost significant aspect to take note is that the method of affixing hidden data into the metadata tags of image file is susceptible and vulnerable to any types of editing or attacks [47]. In addition, any form of appending hidden data can be detected from the file size, which is conspicuous if there is a large data hidden [65].

iii. *Spatial Domain Image Steganography*

An effortless uncomplicated method of embedding within images in digitalised forms is that within the Spatial Domain, where the values of the cover image pixel are modified. To encode the secret information bits, such methods utilise the cover image pixel intensity value levels precisely or circumlocutory. These techniques utilises the most uncomplicated process with regards to the complex embedding and decoding. The implementation of Bit-wise techniques that employ the inserting of bit and manipulating noise through the utilisation of uncomplicated and straightforward mechanisms by Spatial or Image domain or map domain techniques The basic Steganographic systems which are under the Spatial Domain technique consists of Least Significant Bit (LSB), Multiple Bit-planes based, Quantization based, Pixel Value Differencing (PVD), Histogram Shifting, Expansion based, Palette based, Pixel Intensity Modulation based and Pattern based Steganography. Table 3 explains the recent works of Spatial domain methods with a detailed analysis for each method has been mentioned.

Table 2 : The dissimilarity between Steganography methods

Characteristics	Properties	Steganography based domain		
		Spatial domain	Frequency domain	Adaptive Embedding
System type	-	Simple	Complex	Depends on adaptive algorithm
Format dependency	-	Dependent	Independent	Independent
Pixel Manipulation	-	Direct	Indirect (e.g. in transformed coefficient)	Depends on inline technique
Computational complexity	-	Less computation time	Hig computation time	Algorithm-dependent
Embedding Capacity	Payload	High	Limited	Varied
Visual Quality	Imperceptibility	High	Less controllable	Highly controllable
Integrity of visual features	Sharpness, blurring, edges	Maintainable	Less maintainable	Maintainable
Robust	Compression, Noise Cropping, Rotating etc	Highly prone	Less prone	Depends on internal algorithm
Security	Geometric attacks	Vulnerable to geometric attacks	Resistant to geometric attacks	Hard to geometric attacks
Statistical detection attacks analysis	RS, Histogram	Easy to expose/detect	Hard to expose/unsuccessful	Hard to expose/unsuccessful
Non-Structural detection attacks analysis	Non-Structural detection attacks analysis	Difficult/Varied	Easily detectable	Difficult/Varied

i. Least Significant Bit (LSB) steganography:

It is perceived as amongst the effortless and the preferred choice of spatial image Steganographic techniques.The workings of this technique are based on the premise that the least significant bits within an image embody minuscule information and minute modifications in those bits cannot be discerned, and will go undetected by the human eyes. In LSB-based spatial domain techniques, the obscure covert information will be embedded straight within the cover image via the modification of LSBs of specific pixels with no impact on the quality of the original cover image visually, through distortion. By the utilisation of this technique in communications channels, intruders are not able to trace or detect any degradation to the image quality visually, when they launch an attack mode. However, statistic shows traces of noise in the range of 5% of the average bit embedding rate (embedded bits per pixel) created by the embedding process. Previous earlier works in LSB steganography [66,67] had focussed on the system design in enhancing the payload capacity by using a large number of the cover image pixels. After a certain period that passed by, the Steganalysis area of study gained a momentum of strength, to crack into such systems by utilising statistical analysis. After that, in addressing the research problem, researchers were engrossed and have fine-tuned their attention in developing advanced robust LSB methods founded on cryptography-steganography which can avoid such steganalysis onslaughts [68,69].

To enhance the efficiency, numerous researches has ventured into a multitude of enhanced forms image steganography that are based on LSB. LSB matching algorithms were utilised by the significant ones[70]. Adaptive Least Significant Bits inlay founded on features of the image such as texture contents, intensity or edge pixels characteristics[71,72]Optimized LSB substitution are grounded on learning methodologies and others[73,74], In addition, in order to boost the embedding capacity, additionally, the extension of the LSB may cover up to four LSB planes which will yield decreased imperceptibility [75]. Its effortlessness in embedding and decoding process forms the major advantage of the LSB technique. Considering that the majority of formats of the images utilise an 8-bit representation in place of single pixels, the LSBs (normally the sixth to the eighth bit) of a certain number or the totality of the values of the intensity of the pixel belonging to the the cover image are regulated in accordance to the covert information. The LSBs of individual colour planes (Red, Green and Blue) are modified according to each data during the utilisation of a 24-bit colour image which is used as the cover media, Nonetheless, there are slight adjustments that occurred to the stego-image, as the LSB methods are vulnerable to statistical attacks.

ii. Pixel Value Differencing (PVD) Steganography:

It employs the utilisation of concealment of covert information by the comparison of the disparities between the pixel values of a pair of consecutive pixels. Contained within the elementary rudiments of the PVD method [78], during the embedding process, a covert information are segregated from and a cover image into non-overlapping blocks with two neighbouring pixels, and the variant pixel values within individual block which are next inserted into several clusters. The choice of range intervals is chosen in accordance to the manner of the human visual sensitivity to intensity value differences from inferior fidelity to high frequency.

Due to the fact that the PVD shows higher degree of precision as compared to the Least Significant Bits techniques pertaining to the dense embedment performance, on the account that the embedding is smoother during the utilisation of the PVD methods [47]. The configuration of the system design dictates that the modifications is determined within the confines of a particular range interval.

Numerous methods were forwarded through the examination of the pixel correlation in PVD Steganography research area. Various neighbourhood schemes like five, six, seven and eight neighbourhoods are utilised to determine the pixel value differencing, so as to anticipate the ultimate perfect embedment level n the cover pixel [79]. Visual distortions appear to be minute when compared to a majority of alternative PVD methods. The major disadvantage of the Pixel Value Differencing technique is the absence of security, albeit the fact that it produces a more superior image perceptibility factor.

Numerous supplementary security characteristics are incorporated in the typical PVD scheme for the objectives of enhancing this security factor of the Pixel Value Differencing approach. For example, Hussain et al. [80] suggested the utilisation of two methods of embedment procedures for an information hiding technique that enhances security. The respective procedures entail the improved Rightmost Digit Replacement (iRMDR) and Parity-Bit Pixel Value Difference (PBPVD). A further exemplar of enhanced security, histogram analysis based vulnerability PVD [81] is also forwarded . A hybrid embedding schemes were suggested, so as to integrate the benefits of variant embedding schemes, (which are techniques is Steganography that implement the Pixel Value Differencing and Least Significant Bits substitution [82,83]).There has been a huge quantity of researches done on the enhanced forms of image Steganography that are founded on Pixel Value Differencing so as to improve the efficiency. The significant ones utilise Adaptive PVD block by implementing pseudo-random number techniques for choosing the blocks [84] and resolving fall- off boundary issues in PVD by maximising strategy [85] .

iii. Histogram *shifting based steganography:*

The central strategy employed in this method involve shifting the histogram levels of the cover media. The valley (lowest) and peak points (highest) within the cover image histogram is ascertained, which is ensued by the embedding process which involves the alteration of these valley and peak points[86,87] . The method sustains imperceptibility and affords higher payload capacity. The major advantage of the histogram-based image hiding boils down to the scheme's support of reversible data hiding [88] . In addition, it also averts the environment not to exceed grey values of above 255 and below 0 intensity values. In order to evade overflow and underflow issues, and to enhance the data hiding capacity, an optional solution for embedding the maximum and minimum points in the histogram map is suggested by the utilisation of a binary tree structure [89]. Another approach based on histogram shifting imitated method is forwarded as explicated in [90] Rather than using the established reference point selection from the histogram map, this method engages in a process that makes selections based on image pixel intensity. Before the process of embedding, the segregation of the image intensity range executed into non-overlapping segments divisions.. Congruent with the other histogram shifting based techniques, the embedding of the covert data is processed by modifying the peak point pixel intensity with others, within the same segment of the peak. Considering the occurrences of the transformation during the embedment procedure for every single pixel is diminutive, the probability of a multiple layered embedding is viable, that will not undermine the cover image perceptibility, in addition to the flawless covert data recovery. Comparable with alternative methods that are based on histogram, it is a Stegano system that can be reversed, inclusive of the extraction enablement of the cover image in addition to the secret information. The segmented intensity level confines the transformations in the embedding within a secure array that results in high stego-media image quality. The payload capacity is handicapped, as it at the maximum observed to be 0.5 bpp during the evaluation with numerous test images. Additionally however, it is not suitable to be utilised with compressed stego-image, in addition to transmission conduit vulnerable to geometrical distortions such as scaling or containing added noise

iv. Pixel intensity modulation based steganography.

The introduction of the systems of Steganography that are founded on Pixel intensity modulation or adjustment are to serve as a modification of the embedment procedure for pixel intensity adjustment in Steganography based on LSB . In this case, the embedding of the covert information bits are executed within the intensity adjustment in between proximate neighbouring pixels or blocks in the immediate close proximity which is dependent upon the conditions of the embedding scheme. These techniques assist in the provision of improved stego- images quality when compared with LSB modification systems, as a result of the indirect embedding process [91]. Towards the attainment of an enhanced security, edge selection which is based on pixel intensity modulation is suggested in [92]. Towards the purpose of boosting capacity and perceivable quality, additional sophisticated pixel intensity modulation method is explicated in [93].In this instance, the host image sub-blocks houses the embedded secret bits. Smart pixel adjustment guided by the secret data bits will then update the sub block averages. The implementation of adequate thresholds emplaced in maintenance of values adjustments within parameters of the maximum intensity value (overflow).

The procedure of extraction entails the reverse of the embedding phase utilised. Through the review made on these techniques, the evaluation the superiority of the method surpassing the standard LSB modulation method pertaining to imperceptibility, security and robustness. Nonetheless, the other Least Significant Bits systems flaws still prevails, with further investigation required to address the defects.

v. Difference expansion steganography.

It is associated with embedding of covert information over variant pixel pairs. The expansion of the variant values is implemented through the utilisation of divergent techniques, and the embedment of the secret data bits are executed over this expanded difference range [94]. A majority of the difference expansion methods are categorised under the reversible stegano systems, in which case none erroneous extractions of the cover image and secret data are obtained on the receiver's end. A myriad of studies in systems in image steganography that are founded on Difference Expansion were suggested by numerous researchers, and several of the most recent related writings are explicated. In [95], a pre-processing is utilised to avert underflow and overflow issues. It assists in circumventing the circumstances in the event that the possibility that embedded pixels are of higher values as compared to the highest and lowest ranges in the cover image. The Least Significant Bit bits of the cover media are intact, that enables the system to be reversible . The compression of the the Least Significant Bit data bit size is enabled through the application of Huffman coding, and is hidden together with the covert information during the embedding stage. The GAP [96] method-based prediction scheme is utilised for inferring the active embedding portion, The generation of the difference image from the actual cover and predicted cover is then derived.

The embedding of the secret information on top of the expanded form of the actual difference image ensues. The manipulation of the expanded range enables the escalation or reduction of the embedding capacity. The higher the value of the expanded range will result in an increase in the embedding rate, and inverse state of image quality deterioration. Therefore, the expansion range is regulated to maintain a balance between the non perceivability of the image and payload capacity. A threshold implemented in the difference image together with the utilisation of flag bits at high difference values assists in inhibiting the glitches in a harmless interval. Additional steganographic algorithm that is based on difference expansion is explicated by Jung et al. [97]. In this instance, a strategy based on block level difference expansion is utilised additional to an interpolation prediction mechanism. The expansion of the cover image is executed to multiple scales (> 1) and embedding is undertaken as per scale space.

The input images are segregated into sub-blocks at each scale level, and the embedding bits are determined for each expanded sub blocks. The utilisation of the key scaling parameter can enable the adjustments to the embedding capacity. The ascertainment of payload capacity of □4 BPP is executed at a scaling limit of 3 and at a visual quality of □30 dB of PSNR.This technique experiences The vulnerability towards geometrical and statistical attacks, and the entire reversible methods shortcomings is experienced by this technique.

Additional steganography system that is based on high capacity reversible image is cited in writing [98]. The primary procedure is in ascertaining a difference image betwixt the actual cover data and a predicted image grounded on the reference pixels from the cover media. In addition, embedding the erroneous image onto the covert information ensued, and is utilised as the stego-image for communications purposes. Embedment limitation is set by the pixel locations where the difference is situated over the threshold, and this regulation assists in maintaining the system to be flawless from overflow and underflow. On the recipient's end, the reference pixels can be distinguished by the values of pixel, and the pre-arranged configured threshold values. The secret bits are confined through the assistance of the reverse embedding procedure from the stego-image.The central interest is for the embedment not to require a damaging reference peak choice from the histogram map. The rate of embedment can also be altered according to the requirements with consequences of lower visual quality. The overall conclusion entails the confinement of difference expanding techniques to target applications, in which case the cover image is vital and the communications conduit is more robust towards intruder attacks.

Table 3 : The Recent Works Of Spatial Domain Methods

Year	Ref.	Method used	Advantages	Drawback	Result
2017	[67]	LSB	Using a security key to include some cryptography	Low embedding capacity , Poor Robustness against some attacks like (geometric attack and	Maximum capacity for text length is 6 characters

				compression attack)	
2017	[68]	LSB	Higher visual quality , The hiring process possesses high security of the hiring in addition to maintaining the process simpleness based on chaotic sequence	Low embedding capacity , Poor Robustness against compression attack	PSNR = 44.53 BPP = 2
2016	[76]	LSB	· Based on Word hunt puzzle approach. · Reduced modification of per pixel value. · High imperceptibility	Need to test over modern or non-statistical steganalysis	N/A
2017	[77]	LSB	There is a balance between the security and the imperceptibility , Multi-level encryption	· Low embedding capacity. Poor robustness against pepper noise	BPP = ≈1 *PSNR* = >45 dB
2018	[85]	PVD	High embedding capacity , The system has an ability to Averting falling-off boundary issue	Weak security , Low imperceptibility , -Weak robustness combating geometric attack	BPP = 2.483 PSNR = 37.774
2016	[82]	PVD + LSB	High payload capacity., High Imperceptibility	Poor security and poor robustness against attacks ,	BPP = 3.1 PSNR = 40.4
2016	[83]	PVD	High embedding capacity , Simple extraction process	-Poor security and poor Robustness against attacks	Capacity bits = 199,211.2 PSNR = 40.606
2017	[101]	Histogram shifting	High Embedding capacity , High imperceptibility among other Spatial domain techniques	Low security	PSNR = >40
2018	[91]	Pixel Intensities Modulation	Less distortion , High imperceptibility	-Low embedding capacity -Weak security combating noise attacks	BPP = 0.88 PSNR = 40
2016	[110]	Histogram	effective while data transmission , High capacity	Authors didn't mention the robustness	N/A

vi. Multiple bit-planes based steganography.

The method was initiated in 2006 as an extension to the standard LSB substitution method, in which case bit planes were utilised in the concealment of secret data bits [99,100]. Normally, bit plane stegano systems are utilised along with alternative techniques as the entire system performance enhancer [101]. Thus, it is frequently associated with alternative dominant image Steganography classification. A steganography system that is based on bit plane segmentation is charted on the paper [102]. In this instance, the intricacy of individual bit planes is evaluated prior to the embedment procedure. This is ensued by the selection of Bit planes with greater noise value, with associated Hessenberg Matrix are then produced This is followed by the application of the Q-R factorization over this Hessenberg matrix, and the embedding of the secret image sub-blocks on top of the decomposed matrix Q part.

Ensuing the procedure of embedment, the decomposed Q and R parts are integrated, where the stego-image is next produced. In the eventuality of an optimum cover image selection, the resultant effect will be a perfect bit plane choice which enables the embedding of secret bits minus visual quality deterioration. A major system setback entails the possibility of image not being perceived may be nullified in the event of an erroneous. bit slice choice. It also experiences negative impacts as a result of additional flaws derivations related with average LSB technique. In [103] , the authors recommended the said technique through the utilisation of bit planes of pixel intensity values for the secret data wrapping. Phase one involves the slicing of the system into numerous bit planes, with the needed quantity of planes chosen by the utilisation of an ANR255 sequence. In preserving higher security objectives, the encryption of secret data is implemented prior to the actual procedure of embedment. It engages in a 13-bit plane ANR encoder utilisation and the secret data bits are embedded over these expanded bit slices.

Following procedure of embedment, the cover image is reverted to typical 8-bit representation prior to utilising it as the stego-image. The bit plane encoding that has undergone expansion, results in dual benefits. Firstly, it enables the hosting of further secret bits than the typical 8-bit LSB techniques. On another note, there will be a high degree of chaotic embedding, which will result in a more robust system that has a resilient defence system combating intruder's steganalysis process. Additional system benefit entails null necessity for the shared coding system between the interlocutors. The association of the susceptibility of the stego-image to geometrical attacks as a major setback, and the slightest modification of pixel alignment could result in the scrambling of embedded information.

vii. Palette based steganography.

It [104] engages in the utilisation images based on palette to be cover media. Appropriate image formats for this type of approach are PNG, GIF and TIFF. Pseudo random numbers are generated by the utilisation of a secret key and the chosen secret data bit will be inserted on a single cover pixel. In place of the original colour, the colour with the similar parity as the secret bit in the palette is utilised in the embedding process. Typically, palette-based stegano systems can be categorised into two types: Firstly the palette colour is modified to create a distortion within a small range. In such systems, the embedding capacity appears to be small.

The second type maintains the particulars pertaining the colour of the cover data but adjusts the palette entries according to the secret data bits and supports dense embedding. The major interest towards the utilisation of palette-based steganography is due to the lesser comprehensive stego-image distortion in the stego-image in comparison to alternative spatial techniques. The requirement for images to be in specific lossless compression formats forms the main disadvantage of this approach. It is not applicable on commonly used image formats such as JPEG. As a resultant of these setbacks, the approach is less preferred and utilised less for real applications. Imaizumi et al. [105] proposed a dense image embedding scheme that utilises palette based steganographic system which maintains the visual quality at an adequate level for untraceable communications.

This method enables the embedding of multiplex bits of covert data over a single pixel ensuing the evaluation of the difference using Euclidian distance methods, whereby a majority of the palette system is in accordance to the a single bit per pixel scheme. It utilises a parity check for embedding error reduction. A pre-requisite that must be fulfilled in this concealment scheme is the sharing of the mapping positions of the embedding location between the interlocutors to ensure precise retrieval of secret information. In comparison of alternative systems that are based on palette, the payload capacity is on the verge to be considered as large and the visual quality to be higher at approximately PSNR value of □40 dB. For the purpose of obtaining enhanced security characteristics, the choosing of pixels was executed randomly for the embedding procedure[106] .

The procedure of embedding is initiated with the formation of Julia-set fractal images according to the pre-set specified limitations. The extraction of colour channels are implemented, followed by the arrangement of the colour palette respectively. Then, random pixel selection is executed and the palette index is kept up-to-date according to the optimum secret bits match, followed by updating of the stego-image pixel respectively. It is required for the embedding to be shared on the recipient's end and the covert data is extricated by making a comparison between the actual index with the embedding index. This assists in maintaining the visual quality within the array of □60 dB, however, while alternative Steganography features are unaccounted for in this section. The comprehensive evaluation of palette-based steganography is inadequate when taking into consideration advanced LSB steganographic systems. .

viii. Quantization based steganography.

It utilises all types of compression encoding system to conceal covert information bits. The system utilised to encode may be found in various forms of typical codec used for compression such as JPEG, vector quantization and others. Typically, the covert information is segregated into small blocks of data sub samples, which will ensue by embedding these minute data fragments with cover images that are encoded. On the recipient's end, the exact coding is executed onto the stego-image where the retrieval of the covert data is made possible by the utilisation of the inverse embedding process. A steganography system that utilises image, in which case the embedding of the covert data is onto a jpeg encoder is displayed in [107]. For the procedure of compressing, a JPEG coder is utilised that enforces 8 ×8-pixel blocks, where the segregation of the secret information is executed into small parts to be concealed over the transformed coefficients. A multitudinous amount of multiple encoder coefficients may be required by the covert data to house the whole fragmentations. During the compression process, the JPEG coder utilises 8 ×8-pixel blocks where secret data is segregated into minute fragments for concealment purposes over these transformed coefficients. Multiple encoder coefficients may be required by the secret data to host the full fragment. Likewise, the embedding of the whole secret fragments are executed onto a single or additional compression coefficients, whereby on the the recipient's side, a reversal procedure is executed upon the stego-image, with the original form is produced through the compilation of the secret bits. No information is required by the system pertaining to the coefficient location and adaptive selection is influenced by the image statistics to ascertain the embedding location. Authors assert the appropriateness of the method to be utilised with any coders and it offers an added benefit. However, the inadequacy in addressing the geometrical attacks and steganalysis is observed. The explication of a plethora of enhanced forms of quantization-based image steganography are found in the area of research pertaining the improvement of the capacity and reduction to a minimal scale of the distortion. Amongst them, one of the component of this method utilises the modified DCT quantization table for colour image [108] and adaptive hiding steganography based simple optimal quantization [109] .

8. FUTURE TRENDS AND PROSPECT SOLUTION

We have discussed how image steganography algorithms have advanced over a period of time in every domain and have given rise to adaptive steganography. In principle, the key demands in image steganography include hiding secret data in a cover picture so it is less recognizable, be more secure, hard protection from unauthorized access and more capacity in terms of payload. There has been less execution of the mentioned demands even amidst more research work on the same, resulting in unaccomplished achievements. Research notes that even the enhancement of a few characteristics may not positively impact efficiency as there exists a mutual relationship among the steganographic characteristics. The challenge is there lacks a practical solution for resolving all these necessities instantly. For efficient improvement of the present image steganographic approaches, the following steganographic concepts are considered.

i. Steganography based on empirical method lacks a formal connection between the distortion function and statistical detectability which is the important problem in adaptive steganography. It requires development and analysis of advanced coding techniques that are statistics aware.

ii. Research investigations on image steganographic point out stego-image robustness to be the least in parameter considerations. Critically, stego-image has a susceptibility to several attacks from message-passing mechanisms and from unauthorized personnel. Severally, unauthorized personnel easily perform alterations on the characteristics of stego-images which include strength, evenness, etc. The result of this is significant erroneous secret data at the receiver side during retrieval. As a result, there is a need for confirmative alternatives for nullifying the impact of attacks occurring in the stego-media.

iii. The focus should be given to enhance the security of direct embedding by using efficient and less computationally expensive encryption algorithm. This can be achieved by selecting the best cover image and determining the region based on the cover image properties. Use of optimization algorithm such genetic algorithm, game-theoretic approaches along with Markov cover probabilistic distributions could be explored.

iv. Future work could also be aimed at proposing an efficient embedding of secret information in pre cover images which offers higher empirical security. The status of side-informed steganography is limited in the sense that it lacks theoretical analysis. Current work uses the difference between the acquired images (white noise), which is challenging and labor-intensive. Simple and efficient ways need to be formulated.

9. CONCLUSION

Information hiding is an increasingly popular extensive research field that attracts genuine interest in research. This is due to the fact of the rising popularity of steganography in securing data via the network communications. This study encapsulates and forwards the summation on the prevalent image steganography methods in spatial domain,in addition to the analysis made on the various challenges and the setbacks of each individual method which were created in the past years. Every technique is unique and disparate from another. A minority of them engage on the improvement of image quality, meanwhile others are involved on studies related to the capability of the capacity to conceal data or on security issues. On the whole, all of these techniques motivate and enhance endeavours in this field, and is crucial for future steganographic researches. Finally, in conclusion; the open issues entrenched in this study impel and drives the researcher to recommend and promote a cogent resolution to solve this concern .

REFERENCES

[1] HASHIM, MOHAMMED, et al. "A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN." *Journal of Theoretical & Applied Information Technology* 96.4 (2018).

[2] Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." *Signal processing* 90.3 (2010): 727-752.

[3] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." *Computer science review* 13 (2014): 95-113.

[4] HASHIM, MOHAMMED MAHDI, MOHD RAHIM, MOHD SHAFRY. "IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION." Journal of Theoretical & Applied Information Technology 95.19 (2017).

[5] Ahmed, Adnaan, Nitesh Agarwal, and Sabyasachee Banerjee. "Image steganography by closest pixel-pair mapping." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[6] Taha, Mustafa Sabah, et al. "Combination of Steganography and Cryptography: A short Survey." *IOP Conference Series: Materials Science and Engineering*. Vol. 518. No. 5. IOP Publishing, 2019. [7] Muhammad, Khan, et al. "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 (2016): 14867-14893.

[8] Mansour, Romany F., and Elsaid M. Abdelrahim. "An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications." *Multidimensional Systems and Signal Processing* (2017): 1-24.

[9] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." Computer science review 13 (2014): 95-113.

[10] Beroual, Abdesselam, and Imad Fakhri Al-Shaikhli. "A Review of Steganographic Methods and Techniques." *International Journal on Perceptive and Cognitive Computing* 4.1 (2018): 1-6.

[11] Siddiqui, Beenish, and Sudhir Goswami. "A SURVEY ON IMAGE STEGANOGRAPHY USING LSB SUBSTITUTION." (2017).

[12] Sun, Shuliang. "A novel edge based image steganography with 2 k correction and Huffman encoding." Information Processing Letters 116.2 (2016): 93-99.

[13] El-Emam, Nameer N., and Mofleh Al-Diabat. "A novel algorithm for colour image steganography using a new intelligent technique based on three phases." Applied Soft Computing 37 (2015): 830-846.

[14] Srinivasan, B., S. Arunkumar, and K. Rajesh. "A novel approach for color image,

steganography using nubasi and randomized, secret sharing algorithm." Indian Journal of Science and Technology 8.S7 (2015): 228-235.

[15] Rawat, Deepesh, and Vijaya Bhandari. "A steganography technique for hiding image in an image using LSB method for 24 bit color image." *International Journal of Computer Applications* 64.20 (2013).

[16] Dunbar, Bret. "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment." *Sans Institute* 1 (2002).

[17] Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." *Computer* 31.2 (1998): 26-34.

[18] Kumar, Arvind, and Km Pooja. "Steganography-A data hiding technique." *International Journal of Computer Applications* 9.7 (2010): 19-23.

[19] Mishra, Rina, Atish Mishra, and Praveen Bhanodiya. "An edge based image steganography with compression and encryption." *2015 International Conference on Computer, Communication and Control (IC4)*. IEEE, 2015.

[20] Burney, Micaela L. *The History of Steganography and the Threat Posed to the United States and the Rest of the International Community*. Diss. Utica College, 2018.

[21] Hashim, Mohammed Mahdi, et al. "An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching." *International Journal of Engineering & Technology* 7.4 (2018): 4008-4023.

[22] Mahdi, Mohammed Hashim, et al. "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*. Vol. 518. No. 5. IOP Publishing, 2019.

[23] Bashardoost, Morteza, et al. "A Novel Approach to Enhance the Security of the LSB Image Steganography." Research Journal of Applied Sciences, Engineering and Technology 7.19 (2014): 3957-3963.

[24] Yadav, Gyan Singh, and Aparajita Ojha. "Improved security in the genetic algorithm-based image steganography scheme using Hilbert space-filling curve." *The Imaging Science Journal* (2019): 1-11.

[25] Rajalakshmi, K., and K. Mahesh. "Robust secure video steganography using reversible patch-wise code-based embedding." *Multimedia Tools and Applications* 77.20 (2018): 27427-27445.

[26] Manisha, S., and T. Sree Sharmila. "A two-level secure data hiding algorithm for video steganography." *Multidimensional Systems and Signal Processing* (2018): 1-14.

[27] Din, Roshidi, et al. "Evaluating the Feature-Based Technique of Text Steganography Based on Capacity and Time Processing Parameters." *Advanced Science Letters* 24.10 (2018): 7355-7359.

[28] Ciptaningtyas, Henning Titi, Radityo Anggoro, and Muhsin Bayu Aji Fadhillah. "Text Steganography on Sundanese Script using Improved Line Shift Coding." *2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC)*. IEEE, 2018.

[29] Liu, Jie, et al. "Steganalysis of Inactive Voice-Over-IP Frames Based on Poker Test." *Symmetry* 10.8 (2018): 336.

[30] Bobade, Sandip, and Rajeshawari Goudar. "Secure data communication using protocol steganography in IPv6." *2015 International Conference on Computing Communication Control and Automation*. IEEE, 2015.

[31] Han, Chunling, et al. "A new audio steganalysis method based on linear prediction." *Multimedia Tools and Applications*(2018): 1-25.

[32] Nasrullah, Mohammed A. "LSB based audio steganography preserving minimum sample SNR." *International Journal of Electronic Security and Digital Forensics* 10.3 (2018): 311-321.

[33] Hamed, Ghada, et al. "DNA based steganography: survey and analysis for parameters optimization." *Applications of intelligent optimization in biology and medicine*. Springer, Cham, 2016. 47-89.

[34] Malathi, P., et al. "Highly Improved DNA Based Steganography." *Procedia Computer Science* 115 (2017): 651-659.

[35] Khalind, Omed Saleem. *New methods to improve the pixel domain steganography, steganalysis, and simplify the assessment of steganalysis tools*. Diss. University of Portsmouth, 2015.

[36] Cayre, Francois, Caroline Fontaine, and Teddy Furon. "Watermarking security part one: theory." *Security, Steganography, and Watermarking of Multimedia Contents VII*.

Vol. 5681. International Society for Optics and Photonics, 2005.

[37] Fridrich, Jessica, Petr Lisoněk, and David Soukal. "On steganographic embedding efficiency." *International Workshop on Information Hiding*. Springer, Berlin, Heidelberg, 2006.

[38] Muhammad, Khan, et al. "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks." *Future Generation Computer Systems* 86 (2018): 951-960.

[39] Abraham, Ajith, and Marcin Paprzycki. "Significance of steganography on data security." *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.*. Vol. 2. IEEE, 2004.

[40] Gao, Wei, Yongqing Huo, and Yan Qiao. "A security steganography scheme based on hdr image." *arXiv preprint arXiv:1902.10943* (2019).

[41] Davis, Dini. "A Survey on Secret Data Hiding in Quick Response Barcodes." *International Journal* 7.1 (2017).

[42] Qian, Zhenxing, et al. "Robust steganography using texture synthesis." *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Springer, Cham, 2017. 25-33.

[43] Bucerzan, Dominic, and Crina Raţiu. "Testing methods for the efficiency of modern steganography solutions for mobile platforms." *2016 6th International Conference on Computers Communications and Control (ICCCC)*. IEEE, 2016.

[44] Taha, Mustafa Sabah, et al. "Wireless body area network revisited." *International Journal of Engineering & Technology*7.4 (2018): 3494-3504.

[45] Mohsin, A. H., et al. "Real-time medical systems based on human biometric steganography: A systematic review." *Journal of medical systems* 42.12 (2018): 245.

[46] Wazirali, Raniyah Abdullah. *Optimization of perceptual steganography capacity using the human visual system and evolutionary computation*. Diss. 2016.

[47] Anju, P. S., Bineeth Kuriakose, and Vince Paul. "A Survey On Steganographic Methods Used in Information Hiding." International Journal of Science, Engineering and Computer Technology 6.1 (2016): 27.

[48] Zeki, Akram M., Adamu A. Ibrahim, and Azizah A. Manaf. "Steganographic software: analysis and implementation." *International Journal of Computers and Communications* 6.1 (2012): 35-42.

[49] Hu, Donghui, et al. "A novel image steganography method via deep convolutional generative adversarial networks." *IEEE Access* 6 (2018): 38303-38314.

[50] Qin, Xinghong, et al. "A Novel Steganography for Spatial Color Images Based on Pixel Vector Cost." *IEEE Access* 7 (2019): 8834-8846.

[51] Kaur, Sumeet, Savina Bansal, and Rakesh K. Bansal. "Steganography and classification of image steganography techniques." *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2014.

[52] Pillai, Bhagya, et al. "Image steganography method using k-means clustering and encryption techniques." *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2016.

[53] Mohammed, Nada Qasim, Qasim Mohammed Hussein, and Mohammed Sh Ahmed. "Suitability of Using Julia Set Images as a Cover for Hiding Information." *2018 Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology (NTCCIT)*. IEEE, 2018.

[54] Gedkhaw, Eakbodin, Nantinee Soodtoetong, and Mahasak Ketcham. "The Performance of Cover Image Steganography for Hidden Information within Image File using Least Significant bit algorithm." *2018 18th International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 2018.

[55] Ørnager, Susanne, and Haakon Lund. "Images in Social Media: Categorization and Organization of Images and Their Collections." *Synthesis Lectures on Information Concepts, Retrieval, and Services* 10.1 (2018): i-101.

[56] Bai, Junlan, et al. "A high payload steganographic algorithm based on edge detection." *Displays* 46 (2017): 42-51.

[57] Yadav, Gyan Singh, and Aparajita Ojha. "Hamiltonian path based image

steganography scheme with improved imperceptibility and undetectability." *Applied Soft Computing*73 (2018): 497-507.

[58] Thiyagarajan, P., et al. "Pattern based 3D image Steganography." *3D Research* 4.1 (2013): 1.

[59] Elsherif, Salma, et al. "Secure Message Embedding in 3D Images." *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*. IEEE, 2019.

[60] Zeng, Jishen, et al. "Large-scale JPEG image steganalysis using hybrid deep-learning framework." *IEEE Transactions on Information Forensics and Security* 13.5 (2018): 1200-1214.

[61] Feng, Bingwen, et al. "Steganalysis of content-adaptive binary image data hiding." *Journal of Visual Communication and Image Representation* 46 (2017): 119-127.

[62] Sallee, Phil. "Model-based steganography." *International workshop on digital watermarking*. Springer, Berlin, Heidelberg, 2003.

[63] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." *IEEE security & privacy* 99.3 (2003): 32-44.

[64] Alvarez, Paul. "Using extended file information (EXIF) file headers in digital evidence analysis." *International Journal of Digital Evidence* 2.3 (2004): 1-5.

[65] Cole, Eric. *Hiding in plain sight*. Wiley, 2002.

[66] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." *Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205)*. Vol. 3. IEEE, 2001.

[67] Sutaone, M. S., and M. V. Khandare. "Image based steganography using LSB insertion." (2008): 146-151.

[68] Rajendran, Sujarani, and Manivannan Doraipandian. "Chaotic Map Based Random Image Steganography Using LSB Technique." *IJ Network Security* 19.4 (2017): 593-598.

[69] Zhou, Xinyi, et al. "An improved method for LSB based color image steganography combined with cryptography." *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*. IEEE, 2016.

[70] Kadhim, Inas Jawad, et al. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research." *Neurocomputing* 335 (2019): 299-326.

[71] Luo, Weiqi, Fangjun Huang, and Jiwu Huang. "Edge adaptive image steganography based on LSB matching revisited." *IEEE Transactions on information forensics and security* 5.2 (2010): 201-214.

[72] Chakraborty, Soumendu, Anand Singh Jalal, and Charul Bhatnagar. "LSB based non blind predictive edge adaptive image steganography." *Multimedia Tools and Applications*76.6 (2017): 7973-7987.

[73] Bhatt, Santhoshi, et al. "Image steganography and visible watermarking using LSB extraction technique." *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*. IEEE, 2015.

[74] Dadgostar, H., and F. Afsari. "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB." *Journal of information security and applications* 30 (2016): 94-104.

[75] Lu, Tzu-Chuen, Chun-Ya Tseng, and Jhih-Huei Wu. "Dual imaging-based reversible hiding technique using LSB matching." *Signal Processing* 108 (2015): 77-89.

[76] Tavares, Joao Rafael Carneiro, and Francisco Madeiro Bernardino Junior. "Word-Hunt: A LSB steganography method with low expected number of modifications per pixel." *IEEE Latin America Transactions* 14.2 (2016): 1058-1064.

[77] Muhammad, Khan, et al. "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method." *Multimedia Tools and Applications* 76.6 (2017): 8597-8626.

[78] Pan, Feng, Jun Li, and Xiaoyuan Yang. "Image steganography method based on PVD and modulus function." *2011 International Conference on Electronics, Communications and Control (ICECC)*. IEEE, 2011.

[79] Swain, Gandharba, and Saroj Kumar Lenka. "Pixel value differencing steganography using correlation of target pixel with neighboring pixels." *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE, 2015.

[80] Hussain, Mehdi, et al. "A data hiding scheme using parity-bit pixel value differencing and

improved rightmost digit replacement." *Signal Processing: Image Communication* 50 (2017): 44-57.

[81] Zhang, Xinpeng, and Shuozhong Wang. "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security." *Pattern Recognition Letters* 25.3 (2004): 331-339.

[82] Swain, Gandharba. "A steganographic method combining LSB substitution and PVD in a block." *Procedia Computer Science*85 (2016): 39-44.

[83] Kalita, Manashee, and Themrichon Tuithung. "A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution." *2016 International Conference on Systems, Signals and Image Processing (IWSSIP)*. IEEE, 2016.

[84] Hosam, Osama, and Nadhir Ben Halima. "Adaptive block-based pixel value differencing steganography." *Security and Communication Networks* 9.18 (2016): 5036-5050

[85] Grajeda-Marín, Ismael R., et al. "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* 32.01 (2018): 1860010.

[86] Liu, Chiang Lung, and Hsing Han Liu. "Reliable detection of histogram shift-based steganography using payload invariant features." *Applied Mechanics and Materials*. Vol. 284. Trans Tech Publications, 2013.

[87] Qin, Chuan, et al. "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism." *IEEE Transactions on Circuits and Systems for Video Technology* 23.7 (2013): 1109-1118.

[88] Chang, Chin-Chen, Wei-Liang Tai, and Chia-Chen Lin. "A reversible data hiding scheme based on side match vector quantization." *IEEE Transactions on Circuits and Systems for Video Technology* 16.10 (2006): 1301-1308.

[89] Tai, Wei-Liang, Chia-Ming Yeh, and Chin-Chen Chang. "Reversible data hiding based on histogram modification of pixel differences." *IEEE transactions on circuits and systems for video technology* 19.6 (2009): 906-910.

[90] Wang, Z. H., Lee, C. F., & Chang, C. Y. (2013). Histogram-shifting-imitated reversible data hiding. *Journal of systems and software*, *86*(2), 315-323.

[91] Das, Srijan, et al. "A framework for pixel intensity modulation based image steganography." *Progress in Advanced Computing and Intelligent Engineering*. Springer, Singapore, 2018. 3-14.

[92] Islam, Saiful, and Phalguni Gupta. "Robust edge based image steganography through pixel intensity adjustment." *2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS)*. IEEE, 2014.

[93] Yang, Ching-Yu, and Wen-Fong Wang. "Block-based colour image steganography using smart pixel-adjustment." *Genetic and Evolutionary Computing*. Springer, Cham, 2015. 145-154.

[94] Lee, Chin-Feng, Hsing-Ling Chen, and Hao-Kuan Tso. "Embedding capacity raising in reversible data hiding based on prediction of difference expansion." *Journal of Systems and Software* 83.10 (2010): 1864-1872.

[95] Chang, Chin-Chen, Ying-Hsuan Huang, and Tzu-Chuen Lu. "A difference expansion based reversible information hiding scheme with high stego image visual quality." *Multimedia Tools and Applications* 76.10 (2017): 12659-12681.

[96] Wu, Xiaolin, and Nasir Memon. "CALIC-a context based adaptive lossless image codec." *1996 IEEE International Conference on Acoustics, Speech, and Signal Processing Conference Proceedings*. Vol. 4. IEEE, 1996.

[97] Jung, Ki-Hyun. "High-capacity reversible data hiding method using block expansion in digital images." *Journal of Real-Time Image Processing* 14.1 (2018): 159-170.

[98] Lu, Tzu-Chuen, Chin-Chen Chang, and Ying-Hsuan Huang. "High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting." *Multimedia tools and applications* 72.1 (2014): 417-435.

[99] Nguyen, Bui Cong, Sang Moon Yoon, and Heung-Kyu Lee. "Multi bit plane image steganography." *International Workshop on Digital Watermarking*. Springer, Berlin, Heidelberg, 2006.

[100] Ghosh, Uttiya, et al. "Adaptive Multi-bit Image Steganography Using Pixel-Pair Differential Approach." *Progress in Advanced Computing and Intelligent*

Engineering. Springer, Singapore, 2018. 47-56.

[101] Nyeem, Hussain. "Reversible data hiding with image bit-plane slicing." *2017 20th International Conference of Computer and Information Technology (ICCIT).* IEEE, 2017

[102] Banik, Barnali Gupta, and Samir Kumar Bandyopadhyay. "Image Steganography using BitPlane complexity segmentation and hessenberg QR method." *Proceedings of the First International Conference on Intelligent Computing and Communication*. Springer, Singapore, 2017.

[103] Collins, James, and Sos Agaian. "High Capacity Image Steganography using Adjunctive Numerical Representations with Multiple Bit-Plane Decomposition Methods." *arXiv preprint arXiv:1606.02312* (2016).

[104] Niimi, Michiharu, et al. "High capacity and secure digital steganography to palette-based images." *Proceedings. International Conference on Image Processing*. Vol. 2. IEEE, 2002.

[105] Imaizumi, Shoko, and Kei Ozawa. "Multibit embedding algorithm for steganography of palette-based images." *Pacific-Rim Symposium on Image and Video Technology*. Springer, Berlin, Heidelberg, 2013.

[106] Patel, Hetal N., Dipanjali R. Khant, and Darshana Prajapati. "Design of a color palette based image steganography algorithm for fractal images." *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2017.

[107] Seki, Yusuke, et al. "Quantization-based image steganography without data hiding position memorization." *2005 IEEE International Symposium on Circuits and Systems*. IEEE, 2005.

[108] Sachdeva, Sunny, and Amit Kumar. "Colour image steganography based on modified quantization table." *2012 Second International Conference on Advanced Computing & Communication Technologies*. IEEE, 2012.

[109] Sachdeva, Sunny, and Amit Kumar. "Colour image steganography based on modified quantization table." *2012 Second International Conference on Advanced Computing & Communication Technologies*. IEEE, 2012.

[110] Chen, Nai-Kuei, et al. "Reversible watermarking for medical images using histogram shifting with location map reduction." *2016 IEEE International Conference on Industrial Technology (ICIT).* IEEE, 2016.