A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN

[1, 3] MOHAMMED MAHDI HASHIM, [1, 2] MOHD SHAFRY MOHD RAHIM, [1]ALI ABDULRAHEEM ALWAN

[1] Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia

[2] UTM-IRDA Digital Media Center, Faculty of Computing,
University Technology Malaysia, Johor Bahru, Malaysia

[3]Uruk University, Baghdad, Iraq

E-mail: comp.mmh@gmail.com, shafry@utm.my, aliraheem1983@gmail.com

ABSTRACT

Nowadays, information hiding is becoming a helpful technique and fetch more attention due fast growth of using internet, it is applied for sending secret information by using different techniques. Steganography is one of major important technique in information hiding. Steganography is science of concealing the secure information within a carrier object to provide the secure communication though the internet, so that no one can recognize and detect it's except the sender & receiver. In steganography, many various carrier formats can be used such as an image, video, protocol, audio. The digital image is most popular used as a carrier file due its frequency on internet. There are many techniques variable for image steganography, each has own strong and weak points. In this study, we conducted a review of image steganography in spatial domain to explore the term image steganography by reviewing, collecting, synthesizing and analyze the challenges of different studies which related to this area published from 2014 to 2017. The aims of this review is provides an overview of image steganography and comparison between approved studies are discussed according to the pixel selection , payload capacity and embedding algorithm to open important research issues in the future works and obtain a robust method.

Keywords: *Information Hiding, Image Steganography, Least Significant Bit (LSB), Different types of Steganography, Spatial Domain.*

1. INTRODUCTION

In recent years, more research activities have been developed into information hiding because of its gaining importance and due to the increase of digital communication transferred over the network. Information hiding mechanisms can be applied to prevent the secret data from the intruder or the malicious modification. Information Security is procedure of obtaining information secure with more integrity and confidentiality. There are two of information hiding techniques that developed to protect the information and which named Steganography and Watermarking. Both of steganography and watermarking are related to common concept [1][2].

Steganography is a high powerful security provider, steganography can be define as intelligent technique to hide secret data in hosting media to protect it from indiscernible by unauthorized access or the intruder , in a manner of complete silence and deceptive which make hosting media carry the secret data . Steganalysis is detect the secret data by analysis stego media [3][104].

Watermarking is the method of hiding secret data into a carrier media to provide the privacy and integrity of information. This method is used to verify the credibility of the component or to recognize the identity of the digital content's owner. Digital watermark remains same constant even out of manipulation, compression and decompression. Digital Watermarking is divided into two types, visible watermarking and invisible watermarking. Digital watermarking is used for different objectives such as copyright protection, Source tracking, etc. [99][105].

Variety of media carriers that includes audio, text, video image can be used with steganography that will explain later on. Steganography is a strong security provider, especially when it is combined with digital images due of different types of digital image formats that can be used. Image Steganography is the mechanism of hiding the secret data into carrier image. Steganography is interesting especially to applications in which the encryption cannot applied to protect the communication of confidential information. Embedding of image steganography techniques can be classified into spatial domain and transform domain. Special domain plays an important role in all the applications of the image steganography techniques in latest papers, so that the relevant literatures that have been selected in this study emphasizes on this significant subject only by analyzing the main characteristics and the drawbacks also for the image steganography techniques. Steganography is supported many applications such as online transactions, military communication etc. [4][5].

Several review on steganography have been published within recent years, the most important and popular one was published three years ago [109]. it focuses 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 paper 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 [110][111], with respect to the review papers. While the difference in our work summarizes the current image steganography techniques in spatial domain, also analyzed different problems and the drawbacks of each method that have been innovated from last few years.

The fundamental criteria that have been adopted in this review for a comparison between approved studies are discussed according to the pixel selection, capacity and embedding algorithm. The pixel selection is used to achieve the objective of security such as sorting technique [19], Adaptive image segmentation (AIS) [36]. Randomized Secret Sharing (RSS) [26] while the second criteria refers to the Maximum amount of secret message which can be embedded into cover image without retraction of the image quality. Embedding algorithm is used to achieve the objective of image quality (Imperceptibility) which is responsible for keep the quality of the image same of original. This is achieved by keep the pixels value same as original as possible. This work will describe carefully only the spatial domain techniques, transform domain does not include.

The main contribution of this paper is to explore different image steganography techniques in spatial domain during demonstrated , analyzed to the current methods , identify the challenges and open research issues in literature that is interesting in this area.

The remainder of the paper is structured as follows sections: In section 2, Overview of steganography. Steganography techniques describes in section 3. In Section 4, related work is given in details. In section 5, Evaluation criteria of steganography describes in details. In section 6, the challenges and open research issues. Finally in section 7, Conclusion

2. OVERVIEW OF STEGANOGRAPHY

The first description of steganography is used with the Greeks through Herodotus message to the Greeks. Steganography has been used also during the cold war period from USSR and US for security communication. Nowadays, various algorithms are used to protect confidential information along with different media carriers. Generally, a steganography is the process of embedding hidden messages in secret manner that no one, except the sender and purposed receiver(s) can discover the existence of the messages as shown in figure 1. The result will give file called stego object that has the secret message inside it. This stego file is then sent to the receiver side, where the receiver restores the message by applying the extracting algorithm [6]. The figure 1 is shown the general steganography process.

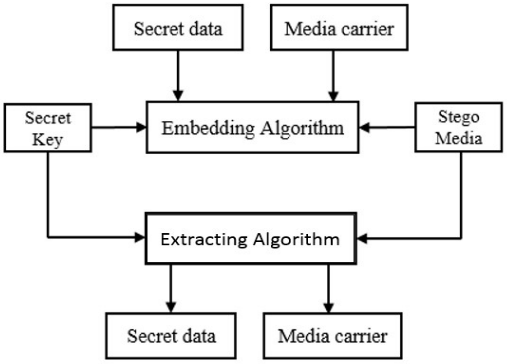

Figure 1. Block diagram of Steganography Process.

The basic model of Steganography consists of three main components:

1- Media carrier: The cover image is also called the cover object that will carry the secret message that will be hidden.

2- Secret data: A secret message can be anything like data, file or image etc.

3- Secret Key: A Secret key is used to encode /decode the hidden message.

4- Stego media (Y): it also called stego object. It is the result obtained after embedding the secret message.

2.1 TYPES OF STEGANOGRAPHY

The steganography is applied practically with all digital file formats but widely perform with digital images because of their frequency on the internet. There are five main categories of file formats which can be used for steganography, as be shown in Figure 2.

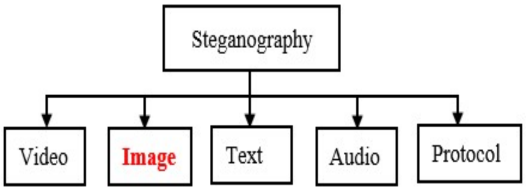

Figure 2. Types of Steganography.

Image Steganography. Digital images are most used as the cover object for Steganography, as well as that are also more popular over the internet. In this technique, a secret message is embedded in a digital image during an algorithm with the help of secret key to create a stego image. Generally, in this technique pixel intensities are used to hide the secret information [7] [103].

Video Steganography. Hiding secret information in a video format is known as video steganography. Video files are consist a collection of images as well as audio. Generally, most of the proposed techniques on images and audio can be implemented to video files too. The use of video Steganography is more eligible instead of the other multimedia files, because of large amount of information that can be hidden inside video format without noticeable by humans because of the continuous flow of information. Many types of video files can used such as H.264, Mp4, MPEG, AVI or other video formats [6].

Text Steganography. Hiding secret information in a text file is known as text steganography. Text steganography requires less memory as it can only store text files. Many formats are used in this technique. In text Steganography number of white spaces, tabs capital letters are used to achieve message hiding. Text steganography is not commonly utilized as text files containing large amount of redundant data [8].

Protocol Steganography. In this technique, the secret information is embedded within network protocols such as TCP, UDP, ICMP, IP etc., where protocol is used as carrier. A network packet consists of packet headers, user data and packet trailers. So during some of the layers of the network model, steganography can be used. This term is known as protocol steganography [10] [106].

3. STEGANOGRAPHIC TECHNIQUES.

Embedding of image steganography techniques can be classified into two classes depends on hosting places and image nature [9].

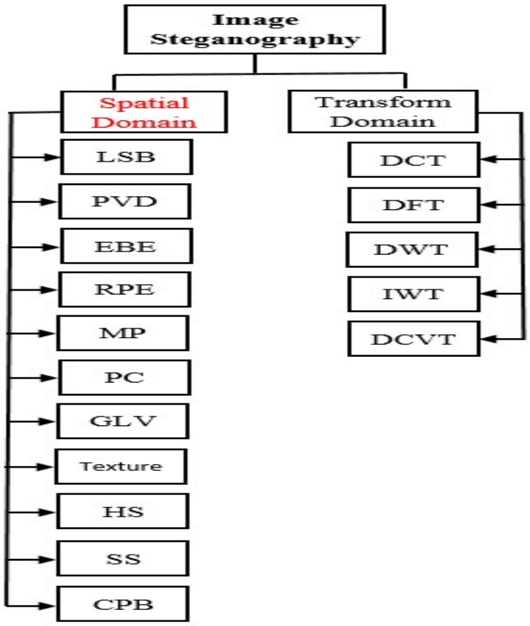

Figure 3. Classification of image steganography techniques.

Table 2 .Differentiation between image steganography technique in spatial and transform domains.

Domain	Advantages	Disadvantages
Spatial Domain	Low computational complexity High embedding capacity High imperceptibility	Vulnerable against the attacks Lacking in statistical analysis techniques
Transform Domain	High security against attacks such as Geometric attacks and compression	High computational complexity Low embedding capacity Lower controllable imperceptibility

3.1 THE FUNDAMENTAL CRITERIA AND SPATIAL DOMAIN TECHNIQUES

Spatial domain or map Domain steganography, the secret information is hided into the cover image by alter the intensity of image pixel values within hiding data directly. Means several image pixel values are converted directly through hiding data using bit insertion with help of bit-wise operation, therefore sometimes characterized as “simple systems”. These techniques classified as following:

Least significant bit LSB- Least Significant Bit is one of most common and easiest technique used in steganography. In this technique, secret bits is hiding within the least significant bits of cover image pixels. Hiding in least significant bit ensures less change in the image pixels value. This technique is generally called LSB substitution [11].

Pixel value differencing PVD - In this technique, two sequential pixels are chosen in order to hiding secret data. Payload capacity of hiding data is determined by checking the difference among two sequential pixels, this is used to distinguish whether the two pixels belongs to an edge area or smooth area [25].

Edge based data embedding technique EBE - This technique works with the edges areas because the human eyes cannot recognize the hiding data within edges areas compared with smooth areas. Therefore, secret data is concealed into pixels around the edges areas of the image. The least significant bits (LSB) technique can be used along with edge technique for more security and Imperceptibility [12].

Random pixel embedding method RPE - In this method, the secret data is embedded randomly to increase the security inside image pixels. Random pixel is generated by using Fibonacci algorithm.

Mapping pixel to hidden data method MP - The mathematical function is applied in this method to embed pixels that based on pixel intensity value and its eight neighbors are chosen according to counter clockwise direction. Embedding data is done by mapping each two or four bits of the secret bits within each of the neighbor pixel based on features of the pixel [100].

Pixel connectivity method PC - In this method the cover image is transferred into binary form and then labelled using the 4 connectivity or the 8-connectivity method. A group of pixels, which is connected vertically, horizontally or diagonally based on Connectivity types, called an object [101].

Gray level modification GLV - First proposed of this method was in 2004 by potdar et al. this method is used to map data (not embed or hide it) by modifying the gray level values. This technique uses the concept of odd and even numbers to map data within an image. by mathematical function , pixels are selected From a given cover image .The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image [14].

Texture based method (Texture) - In this method, the secret and cover images are divided into blocks of specific size and each block in secret image is taken as a texture style for which the most similar block is found among the blocks of the cover image. The embedding execution is carried on by replacing these small blocks of the secret image with blocks in cover image in such a way that least distortion would be imposed on it [95].

Histogram shifting methods (HS) - To hide secret message into cover image histogram will be used. In this method location of the pixels used to embed the secret message that is represented by histogram that generated using shifting process of the histogram. Histogram related with frequency of the pixels in cover image, so generating of histogram most of the pixels have least frequent will determined. To determine the different frequency (high or low) raster scan is used in this method. In term of histogram, the embedding will happen in the high or low peak point. The disadvantage of this method is capacity limitation [66].

Spread Spectrum Method (SS) - This method takes different action in embedding selection, wide band of frequencies took over the signal in bandwidth of communication. New modulation choosing spread the frequency of the pixel used here as a white noise to modulating the narrowband. During spread, the noise over frequency the energy of narrowband signal will reduce. In this case, the signal become easy to detect and the embedding behave like Gaussian noise on the image. Distortion of low noise cannot be recognising by naked eye so embedding in this area is useful. Spectrum of secret embedding is spread multiplicatively of the hiding data suggested by (Valizadeh and Wang, 2012) to predict the error in capacity and security channel. Due to dealing with host signal this method is worth with watermark rather than steganography for frequency dependence reason [15].

Color Palette Based (CPB) method - Color image behold in this method by inserting bit in every color pixel. Random function generates the numbers and these numbers reflected the pixels that hold the secret bits. Stego key stores these pixels numbers to use in extraction process for other part (receiver). Choosing or selecting pixels searching the nearest colors that are not affected during embedding. High level of security produced in this method because of random algorithm dependency (Wang *et al.,* 2005). 24 bits represent the RGB pixel and 3 bits that host the secret message by algorithm of cycle color. This method more robust against statistical attack than sequential embeds method [102].

4. RELATED WORK

In this study, we conducted a review of image steganography in spatial domain to explore the term of steganography by reviewing, collecting and synthesizing different studies that related to this area published from 2014 to 2017.

Al-Dmour et al. have used edge area detection area and XOR function instead smooth area in a cover image to stop against HVS. This algorithm is dividing the image into non-overlapping blocks that would be individually evaluated to get the edges area. Sensitivity of edge area allows hidden bits to eclipsed form HVS attack will become less sensitive in this area. Illumination of pixels in edge area will be different from this point zap to design new steganography system [9].

Genetic Algorithm (GA) based on a tunable visual image quality was introduced by Kanan, and Nazeri (2014). Lossless data in special domain was used to optimize problems in steganography. Experimental results show high embedded capacity with enhanced PSNR [13].

Al-Tamimi et al. suggested a novel method embedding for color image steganography by using Least Significant Bits (LSBs). The proposed scheme has three levels of security, the various number of possible stego-keys, and random pixel selection of first pixel where the hiding process starts and the transposition applied to each 24-bit block of the message to be embed. The embedding process start from first pixel position is calculate by using stego key [16].

An image secret sharing scheme using lossy compression and Arnold transform (AT) for grayscale images has been proposed by Das et al. The secret image is encoded by block based on lossy compression technique. Arnold transform is applying on each sub-image to obtain the scrambled sub-images in order to increase the security level and then shares are generated with the help of Shamir's secret sharing [17].

Das et al. have mentioned that a new technique of image steganography to concealing multiple secret images in a single 24-bit cover image based on LSB substitution and Arnold Transform. This method introduced a technique of multiple image hiding inside a single color image of 24 bit using Arnold transform taking three 8-bit secret images. The proposed method gives the Low computational complexity and high capacity compared to method [18].

A new approach proposed by [19], a spatial domain steganography method to conceal secret data inside the image based on canny edge detector and 2k correction. This approach used Huffman encoding and coherent bit length to compress the secret message. In order to improve security, sorting technique is utilizes to randomize the edge pixels. This approach provides high security with enhanced PSNR.

An enhanced data hiding method by simple LSB substitution with an optimal LSBs method relied on spatial domain, proposed by Mohamed et al. The image is divided into two parts, one for embedding the secret message and applies change to the value of some bits that have the secret bits obtained by the simple form of LSB substitution technique. The other part is used to indicate which change is applied to each pixel exist in the first part. The experimental results show that the proposed method provides larger embedding capacity and better image quality [20].

Secure Image steganography through The EMD (Exploiting Modification Direction) and spatial domain has done by Kuo et al. The proposed scheme has two main contribution make the system more effective. First is only n/2 pixels will be modified and the value is +1 or −1 when the group has n pixels. Secondly, the embedded capacity maintains at least 1 bpp when n is increasing. The cover image is divided into non-overlapping blocks by scanning each line of pixel from left to right and top to down manner to obtain optimal n-tuples to hide the secret message [21].

Rakesh Nayak et al. have used a new approach based on the combination of the steganography and cryptography. The new method mainly focused on security by apply Bit stuffing BSS technique on secret message to inserting non information bits into data to break up bit patterns to affect the synchronous transmission of information and then used the RSA algorithm to encrypts the secret message . The cipher text is embedded by using LSB insertion technique [22].

Muhammad et al. the authors presented an imperceptible image steganographic scheme within spatial domain for grayscale images. The pattern based bits shuffling algorithm (PBSA) is used to encrypted and shuffled the secret data with secret key helping . While embedding encrypted data is done by M - LSB method in the cover image, hence making its extraction relatively more difficult for attackers. In this paper, results is evaluated by qualitative and quantitative analysis [23].

An enhanced edge steganography approach for data hiding methodology is given by Mungmode et al. In this technique, the LSBMR and threshold value is used to improve the quality of an image and modification rate of stego image. Embedding process is used the threshold value in RGB components of the cover image as a parameter for selecting the optimal frequency pixels and then hiding the secret data with the help of LSBMR algorithm. This method provides around 0.2 to 0.6 % of enhancement in the image quality and achieves around 4 to 10 % of enhancement in the amendment rate of an image compared to Sobel and Canny edge detection techniques [24].

Three levels of security is explained by a new scheme to hide secret message into a color Image. First layer, Advanced Encryption Standard (AES) algorithm is used to encrypt the secret message by accepting a 128-bit secret key. Generating number of segments with different dimensions of an input cover image by accepting the same secret key by using NUBASI algorithm and this is the second layer. Last layer of security is by embedding the secret message into the segmented image by using Randomized Secret Sharing (RSS) algorithm [26].

Sahib Khan et al. have used new study to implementation of VLSB steganography, where variable numbers of bits for gray scale image is used. The proposed study is called varying index varying bits substitution (VIVBS). The aims of this paper is to overcome the drawback of DDDB and MDT methods in terms of SNR, MSE, and PSNR where these terms still not achieved as a perfect result. The proposed scheme is defines how much data which need to hidden in a pixel with specific index by calculated either x-intercept or y-intercept of pixel positions in cover image. The size of proposed key can be changed by changing the range of LSB used. In VIVBS algorithm, each pixel is processed and hiding a number of bits into pixel is depending to its index number [27].

Thakur et al. have carried out a novel security method based on image Steganography with cryptograph to hide secret image. The idea of the presented method is to encrypt the secret image using the proposed encryption scheme at first and then hides the encrypted image by Steganography scheme. The algorithm consists of two main sections. The first is to proposed encryption technique to encrypt the confidential image based on symmetric key concept. The second uses Steganography technique to hide the encrypted image using randomization techniques and LSB insertion [28].

Color image steganography system using hash function and edge detection technique in spatial domain has proposed by Singh et al. The canny edge has been applied on color image as a Edge detection method and then hash function algorithm is used to hide text message into the image. The proposed scheme can be applied on different types of image formats like-jpg, jpeg, bmp, tiff etc. [29]

Patel et al et al. have implemented and analyzed the steganography method and AES algorithm to make the evaluation and comparison into different formats of Images and gives the most suitable information with this technique. They are used LSB substitution algorithm in order to implementation Steganography method. This analysis and the evaluation is done with different parameters such as delay, PSNR, MSE, and Absolute Mean Square Error (RMSE) [30].

A new reversible data hiding technique using Pixel Value Difference (PVD) and Difference Expansion (DE) has introduced by Jana et al. The secret message is first divided into sub-stream of size n bits with proposed technique. Pixel Value Differencing (PVD) has been used to embed n−1 bits and 1 bit is embedded using Difference Expansion (DE). Finally, according to shared secret key bit stream, these the two-stego pixel pairs are distributing among dual image. The extract technique is the same embed technique in reverse sense [31].

Secure color image steganography through least significant bits (LSBs) has suggested by Al-Tamimi et al. Asymmetric key for image steganography is utilized in this scheme which is an array of 32 integers. Data hiding is inserted randomly according to pixel selection generator and in hiding message; the transposition is applied to each 24-bit block. This helped to improved security on LSB substitution method [32].

A General Exploiting Modification Direction GEMD-map scheme has been proposed by Kuo et al. The objective of present work is increase capacity by reduced spatial redundancy in cover image. The cover image is partitioned into non-overlapping blocks based on scanning left to right and top to down pixels and partitions the secret message for each block using OGEs function [33].

A method for image steganography based on a combination of Cryptography and steganography has been described by Das. The objective of this research is using LSB substitution to hide multiple secret images in a single 24-bit. Before embedding, each message is encrypted using Arnold Transform (AT) algorithm. The first three MSB bits of the first encrypted secret image is embedded randomly in the last three LSB bits of the red pixels and then first three MSB bits of the second and third encrypted secret image is embedded randomly in the last three LSB bits of the green and blue pixels respectively. The Stego-image is generated by combined the modified pixels [34].

Bhatt et al. Have used basic terminologies of image steganography and Visible Watermarking based on LSB Extraction Technique and Scale Invariant Feature Transform (SIFT). The ensures combination of both gives multiple layers of security and will achieve requirements like capacity, security and robustness [35].

A robust image steganography based on adaptive neural network with Genetic Algorithm has been proposed by El-Emama. The proposed system is more complexity to implementation due the deferent layers of security. The SPIHT algorithm has been applied to compress the secret message and then encrypted it using AES algorithm. Adaptive image segmentation (AIS) is used in this system as a new adaptive image segmentation, this adaptive used to hide data randomly instead of sequentially [36].

In another method, a new scheme used to hiding information in order to comparing with LSB technique called DKL, has suggested by Udhayavene et al., where both LSB and DKL algorithms is evaluated by using basis evaluation such as MSE, PSNR, Relative Payload and Rate of Embedding. The proposed work is implemented by using S-tool, which successfully hide the data inside an image. In this work, different image format is supported with this tool such as BMP, WAV and GIF [37].

Khamy et al. have proposed a new steganography technique to minimize and solve the distortion on the stego -image. The proposed work is used two LSB steganography algorithms based on NEQR. The cover image is divided into blocks and each block, hides one secret message bit. In first LSB algorithm , which embeds secret message bit by replacing the LSB's bits of the cover image with the secret message bits directly and then second LSB algorithm is block LSB which embeds a secret message bit into a number of pixels that belong to one image block [38].

In order to design an effective image steganography system to safe data transfer scheme over Internet, Patil et al. has embedded secret data using Bits Difference Based on Most Significant Bit (MSB) technique. Bit no.5 is used to store the secret bits based on the difference of bit No. 5 and 6 of cover image. The result of proposed work is secure and computationally efficient as well because of using MSB [39].

Devaraj et al. have used LSB substitution nonlinear riotous calculation (NCA) and DCT to suggest a chaotic algorithm. This algorithm is used to hide secret image into cover image where NCA is used to observation capacity and before embedding DCT is apply on secret message to increase the security. Three bits can be used to hide with every pixel inside the LSBs of every byte of a 24-bit image. The simple LSB algorithm is used to hide the message with helping from secret key [40].

Cemal Kocak has suggested a Couple Layered Security Model CLSM using a hybrid structure of cryptography and steganography. The cryptography procedure for secret message through using a 16 character (128-bit) keyword that provides a higher level of security. The encrypted message has been embedded using two bits in LSB substitution algorithm for G and B channels of RGB. CLSM scheme show a better results by compared to Pixel Value Differencing method and other methods [41].

An improved image steganography method based on two methods to embed the secret image into parallel images. The idea of this paper is to increase the security with large payload capacity by using parallel images. The embedding process is achieved by calculating the cost of embedding in each pixel by suitably distortion function and then secret message is embedded depending to cost. The proposed work can be improved security based on cost embedding [42].

A new approach towards the key generation to conceal secret data into an image based on edge detection and HSI color model has been introduced by Yadav et al. The Canny edge detection has been applied to fetch a true edge with threshold area and then 2LSB procedure is used for embedding. In HSI color model can hide large amount of information with compare to grayscale images. This method is used RGB, and binary images. The results show high security and capacity [43].

Bukhari et al. Used a chaotic map encryption along with grey scale image steganography . The first phase is the grey scale image encryption where the Arnold cat map has applied as a chaotic map that gives randomizations in the original image to enhance the security. The second phase is the embedding phase is done by using least significant bits of the cover image to hide the encrypt message. Finally, generates the stego image with helping from stego-Key [44].

Al-Omari et al. have done RGB coloring model for secure data where secret message is replaced by positions of image pixels utilizing predefined character-color mapping and the color value of pixel. The secret message bits is distributed randomly in cover image with helping of key, this work is achieved within the embedding process. This scheme provides a better quality and robust stego images that resists against statistical attacks [45].

Sharma et al. have proposed a method to overcome the limitation of time, robustness and distortion in image steganography called the zero distortion technique (ZDT). Different file formats were performed with this method. In order to enhance security, the chaotic sequence was employed as encryption algorithm for a better randomize. The method can be considered as efficient algorithm in terms of time, capacity in comparison to LSB existing technique [46].

A novel image steganography algorithm based on LSB and Edge detection has proposed by Chaturvedi et al. The main idea of the presented work is to hiding the data in the 2-bits LSB of the edge pixels only. The Canny Edge detection method was employed to distinguish the true edge pixels. This method can be applied for various gray scale images with comparison on existing and proposed scheme. The PSNR value was evaluated by compared for EG-LSB and other techniques [47].

Gulve et al. have used a code conversion to improve the steganographic system performance. This method mainly focused on modify the pixel difference value (PVD) where modification is done before hiding the secret data. Here, the cover image is dividing into 2 x 3 block of pixels and average (N) is calculated of the bits which can be hidden in five pairs of that block and then converting the secret data into gray code before embedding to generated the stego image. Result achieved a better hiding capacity and improved quality of stego image [48].

Vidya et al. have proposed a novel image steganography algorithm based on Ken Ken puzzle in the spatial domain. The proposed scheme is carried out one of mathematical puzzle as Sudoku named the Ken-Ken puzzle. The Ken Ken scheme is constructed from a Sudoku scheme, but with extraction process, the Ken Ken scheme has to be reconstructed by the intended extractor. This algorithm has been compared with existing Sudoku scheme using several statistical evaluation such as PSNR, Average Difference (AD) and Maximum Difference (MD) [49].

Gandharba Swain has suggest nine pixel differencing with modification of Least Significant Bit (LSB) substitution and pixel value differences (PVD) to get high embedding capacity with a better imperceptibility. The proposed method design is start with dividing the cover image into 3×3 non-overlapping blocks. based on average of pixel value differences in nine-pixel blocks , the security has been addressed by hiding variable number of bits in different blocks using categorizing the blocks into one of the four levels (lower, lower-middle, higher-middle, and higher). The random selection positions is used to enhance security in this scheme. The extraction can be applied simply using the 2LSBs of the 9th pixel in every 3 × 3 block [50].

According to Roy research, the input is a carrier image and secret message and the output is stego-image. The scheme process was started with converting the secret message into binary code and then calculating its size. In this algorithm image is partitioned into non-overlapping blocks and Find smooth and textured areas inside the block using the individual entropies. Variable embedding rate data hiding scheme is ensured both smooth and textured areas in the cover image and this can be optimally used with high embedding efficiency. The method is shown optimally results in terms of stego- image fidelity and statistical imperceptibility [51].

According to the fact of achieving higher levels of security for data transmission, solution is to combine of Cryptography and Steganography has proposed by Ajin P Thomas et al. In this method, the secret message is encrypted using Vernam cipher algorithms and then embed the cipher message dynamicity into an image by transforms cipher message into bytes and divides each byte into pairs of bits and assigns the decimal values to each pair, which is known as a master variable. The master variable value, hide the cipher message into Least Significant Bit location, such as 6LSB and 7LSB bit or 7LSB and 8LSB bit location or 7LSB and 6LSB or 8LSB and 7LSB bit location [52].

A new method based on a combination of cryptography and steganographic to improve the secure steganographic system performance. The cryptography scheme is done by using the Caesar‟s algorithm to encrypt the secret message and then LSB algorithm is used to hide the encrypted message within an image though private key [53].

In order to enhance the security of image steganographic a new method has been proposed known as mosaic image steganography based on genetic algorithm and key random permutation. The concept of mosaic steganography was proposed by

Lai and Tsai (2011). In this method, genetic algorithm reduces the computational complexity in terms of time complexity, space complexity, used to generate mapping sequence, security and robustness enhances [54].

A new methodology has been suggested for image steganography. In this work the cover image is read and segmented into RGB channels and then if the 8th bit of the pixel are matched with the secret bit the pixel position of the image is noted in a separate file. The G component is chosen for pixel matching in this work and if the secret message contains large capacity so the red and the blue component can be used also .In other method to effectively secure the e-banking system that has proposed by Devadiga et al. based on combination of cryptography, steganography technology and data mining. This method is carried out the transaction using this image for more security as compared to the existing method [55-56].

A new method of hiding data proposed based on steganography conjunction along with cryptography this method is named dual steganography. The main aim of this method is to present two level of security using two cover images and two different stego keys. In first cover image is using 4-bit LSB algorithm to hide secret data with help from stego key 1, the stego image 1 is generated as a result. Then the stego image 1 is considered as the secret data and embedding it within cover image 2 using 4-bit LSB algorithm also by helping from stego key 2. At the end, the stego image is generated [57].

A payment system for online shopping has been introduced by Rajendran et al. to embedding secret text within colored image of any size using spatial domain. The proposed method is used the combination of steganography, visual cryptography and LSB encryption. The experimental result is improved the steganographic system performance [58].

Klim et al. have improved a high payload capacity method based on selected least significant bit SLSB that is applied on color images. The magic square order is applied to scattered among the image pixels and secret bits and then using SLSB value for embedding. This method is works on square image dimension only and this is a weak point. The results are measured using PSNR, MSE, Correlation and Histogram [59].

The combined both steganography, cryptography and genetic algorithm to give greater security with ensure improvement in the steganography performance. The experiments result have been shown the efficacy of the developed system. In other method, a new modified LSB technique suggested for Image Steganography to hide the secret data. In this scheme, LSB technique is improved so files which have comparatively large size as compared to text file can be hidden successfully [60-61].

Alsarayreh et al. have proposed a novel image steganography system utilizing the exact matching between the image's pixel and the secret text values. The secret text is transform to ASCII representation and then Blue channel value is selected in an image in order to matching with the secret text value this is done by brute force algorithm. The random key–dependent data (RKDD) is utilized as a part of the separating procedure. The proposed system is abbreviated as EM-RKDD [62].

A new design to improve the Imperceptibility of the stego images based on an adaptive embedding technique. The new scheme offers different levels of complexity by using multi-resolution analysis to ensure improvement in the steganography performance. The multi-resolution analysis are segmented into three levels and each level is assigned different complexity measure, namely CPX1 and CPX2 regions. The CPX2 region is used to hide the secret data via LSB algorithm [63].

Sharif et al. proposed a robust image steganography via three-dimensional chaotic map LCA map along with strong chaotic characteristics and high maximum Lyapunov exponent 20.58. In the proposed scheme strong chaotic is used to random selection with length of 2L and L is the length of secret message. The embedding process is used both LSBs and MSBs with three high level chaotic maps to select of desirable pairs to hide the secret message [64].

Mocanu et al have proposed a new robust approach based on image steganography with the help of cryptography algorithm. The Boolean algebra and trigonometry are used to obtain this algorithm that used to modify on pixel level with helping from encryption key. The encryption key can be obtained by RSA algorithm. The encryption algorithm proposed in this research it was necessary to create a matrix containing pseudorandom values [65].

Rashid et al. introduced an image steganography scheme based on LSB matching and LSB substitution scheme to embed secret data within an image. The advantages of LSB is shown in this scheme in order to increase the capacity while obtain a better image quality. Both of grayscale and color images are used in this method. This scheme is called robust increased capacity image steganographic scheme RICISS and the security analysis and robust analysis is carried out of this scheme [67].

Based on optimal pixel adjustment process OPAP, Gupta et al. have carried out an image steganography technique where the secret data is hiding into the moderately higher significant bits. In this scheme, color image is used. The proposed embedding scheme is used higher order bits for embedding and therefore to stop distortion of the stego-image, authors mathematically restrict the amount of distortion to a maximum value 4. For this, two groups of pixels are maintained which are used for selecting the pixels for 4th or 5th bit embedding [68].

An improved in transparency and security on previous work of LSBMR with no need to another object, this method called ILSBMR. This method is hiding the secret message into cover image using the modification of LSBMR method. To this end, the cover image is divided into blocks and then chosen the best block to embed secret bits by using LSBMR. In order to increase security of the secret message, all bits are XORed with LSB (B) and then they are placed in the blocks created [69].

A secure crystographic has been presented to secure the secret messages in social media based on MS-directed LSB substitution, HSI color space, secret key and TLEA. The TLEA is applied to encrypt secret information before embedding and HSI color model is used for message concealment based on MS to prove security and imperceptibility. Finally, encrypted information is embedding using MS-directed LSB substitution method with random distribution bits in different areas of the cover image. The qualitative and quantitative results achieved a better performance of the proposed work [70].

Khan et al. have presented a secure image steganographic scheme based on SKA-LSB substitution method along with multi-level of cryptography. The stego key is encrypted by a two-level encryption algorithm TLEA where a multi-level encryption algorithm MLEA is applied to encrypt the secret data and then encrypted data is embedded into an image using an adaptive LSB substitution method with helping of stego key [71].

Islam et al. presented a novel data hiding process using edges technique and LSB substitution technique. The canny edge detection technique has been used to get true edges into gray scale images. The edges selection for hiding is conditional on the length of payload capacity and the image. The proposed method is used two bits of LSB substitution for embedding in an image. In this work pseudo random number generator PRNG is used created random secret message [72].

Baghel et al. have used dynamic programming method to improve the payload capacity and suitable image quality based on Image steganography. The dynamic programming is used to calculate cost based on energy where this cost and energy is used to select pixels randomly. The proposed method is simulated and mean square error and peak signal to noise ratio is calculated [73].

In order to carry out an effective and secure algorithm in colored image steganography based on sparse matrix encoding, Vipul shah is implemented a LSB algorithm along with sparse encoded matrix in this method that hide the data such as secret key this useful to enhance the security of system [74].

A new symmetric key based on image steganography technique has introduced by Rajendran et al. the pixel position has been chosen randomly to hide secret bits. The main issue of proposed system is to selected pixel position randomly from cover image using chaotic map to increase the efficiency and security. Four different grayscale images are used for testing and prove the performance of proposed system [75].

A new enhance approach of information security in RGB Color Images based on steganography technique and hybrid feature detection technique has suggested by Juneja et al. the objective of this approach is to improve LSB based steganography technique with high security where LSB substitution and adaptive LSB substitution technique have been used to hide data. The detector technique integrating Canny and Enhanced Hough transform for bifurcating an image into edge and smooth areas. Before embedding process secret text is encrypted using the advanced encryption standard [76].

A random key generation and raster scan for steganographic have been presented to improve security of the system. The original image pixels is scanning to support the security level of the secret text to be hidden. In this paper an optimal pixel adjustment process OPAP is applied to obtain a better image quality. Before embedding the secret text is converted to integers by using extended binary coded decimal interchange code EBCDIC, followed by permutation using the key. Finally, stego-image is generated by using NOR (XNOR) operation with the secret key [77].

Sehgal et al. suggested a novel method to hide the secret message into an image with describe the different pros and cons by another authors. The general method has three phases secret sharing phase, steganography phase and data extraction phase. The secret sharing phase is used to distribute secret data between the shares and then shares are embedding into an images within steganography phase. The extraction phase is revers of up process [78].

Different carrier of image steganography used to encrypt the secret data proposed by Sneha Bansod and Gunjan Bhure (2014). The secure data is hidden using some JPEG or BMP images, which may be more helpful in this case and to keep the data safe. The LSB modification is used to embed the secret data [79].

Secure image steganography through Image Steganography for Criminal Cases (ISCC) technique has done by Suryawanshi et al. The proposed method is used to maintain the privacy and confidentiality of the data where the secret key is applied to encryption and decryption the secret data. The secret key is generate by the Rijndael Algorithm (1998) [80].

Imran Khan used a methodology to provide large capacity with maintain image quality for novel steganographic method based on neural network along with random selection of edged areas. This scheme divided the image into non-overlapping blocks and each block used to generates a number of edged regions. All these blocks are created by employ PVD differencing method. Before embedding a neural network is implement to obtain a stego-image. This paper concludes of proposed method is more efficient and more security [81].

Manaseer et al. proposed and tested a colored image steganography for embedding the secret message based on reference and two LSB algorithm versions where the versions called plain LSB and condition based LSB version. The main core of this work is to hide message within JPG image format after dividing it into (R, G, B) matrices, then hiding information in the reference of the data. The proposed work is high security by compared with others method according to reference of data [82].

Yang Rener et al et al. have proposed a new image steganography technique along with pre-processing of DES encryption technique to improve high security. The secret information is encrypted by applied the DES encryption technique and then LSB steganography is used to hiding the encrypted information. Experimental result of the system is obtain a higher anti-detection execution [83].

A new improvement method of LSB algorithm based on bit inversion schemes has introduced by Zeghid et al. Two LSB schemes of the method are applied to enhance the security more than more than plain LSB method. In these techniques some pixels of cover image are inverted in LSBs if they come within a specific pattern of some bits in the pixels. The new scheme offers high security and the bit inversion technique can be joint with other techniques to enhance the steganography further [84].

Huang et al. have suggest an improved version of Ou and Sun’s (2014) to increase the hiding capacity. In proposed scheme two secret message has been used based on absolute moment block truncation coding AMBTC where one of these secret message is used to embedding into the complex blocks and the second embed into smooth blocks. Result show high image quality higher than Ou and Sun’s method [85].

Aydogan et al. have proposed a new methodology of image steganography via block matching and LSB algorithm to hide the patient data within medical images. This scheme is employed to ensuring as minimize bit changes as possible where eight scanning orders are applied in a block matching and six of these scanning orders are newly implemented. The stegdetect tool is used to test the proposed method. The data hiding is achieved a better robustness in this method [86].

An online voting system based on steganography and visual cryptography has suggest by Rura et al [87]. In the proposed system techniques, the password hashed based on visual cryptography, image steganography and threshold decryption cryptosystem. To achieve a better idea and objectives of this proposed, the Software Development Life Cycle (SDLC) was used to carry out the eVote system. The SDLC method is known as the waterfall method. The suggest system is applied in Java EE with MySQL database server.

Chakraborty et al. proposed an Edge Adaptive image steganography to embed the payload capacity based on modified median edge detector MMED. In the proposed scheme cover image is transformed into predictive error image with same size using MMED algorithm and then divided the predictive error image into non-overlapping blocks of Z×Z pixels. Before embedding, secret message is divided into three parts with names S1, S2 and S3 and then embed these parts in chosen area based edge adaptive. The edge adaptive proposed increases the embedding capacity with minimize the detection property [88].

Bajpai et al. have used two stages to construct a secure system with high payload capacity for image steganography. First stage of proposed work is generate the mottled image from a chosen image through morphing it and second stage embed the secure text using bitwise operators with multi-keys to enhance security [89].

According to Bandyopadhyay et al. a novel adaptive technique for constructing a secure data hiding technique in digital images where the secure data is encrypt using chaos theory system before embedding. A secure LSB algorithm is used in the scheme that helps to increase the security thought the non-linear dynamic system (chaos). Embedding procedure, secret image is Break into eight parts and then each of the eight parts will be generate a bit sequence with encrypt all bits of the secret image. Finally, the encrypted eight bits is embedded into four bits of LSB algorithm respectively and this operation will stop until embedded all the bits of encrypted secret image [90].

Integrate cryptography and steganography in order to secure the private patient data into medical image introduced by Al-Saiyd. In this work, random numbers are generated from primitive roots of prime numbers that are used in cryptography and steganography procedures. The block-ciphering algorithm is implemented to protect the patient data using the random numbers which is generated and then embed the encrypted data into 2LSBs of Blue and Alpha channels of the medical images. During the process of encrypting the patient data and embedding it, random keys is generated to increases the cost and the complexity of the method. The proposed method is used medical image with PNG format [91].

Hajduk et al. have used a novel cover selection steganographic method to obtain an optimal cover image for a secret message from database. The idea of this article is to overcome the drawback of time consumption in cover image selection and the basic embedding methods is used. At the end , the method is achieved a better efficiency with decrease the secret message to 70% of original vector length and then time consumption decreased by half whereas the difference was only by 0.24% [92].

Yu et al. have proposed a steganographic algorithm via LSB and the second least significant bits SLSBs that is used to increase payload capacity with low change rate. The method is employed to modify one pixel when three bits of secret message is used to hide into three pixels of image. The embedding procedure, local texture is defined in this algorithm and then the image is divided into blocks that size m×n with no overlap, and the texture of a block is used to hide the secret message. The proposed work is compared to other steganographic algorithms such as LSB, LSBMR, EPES and the result showed that the proposed algorithm improved security and high payload capacity [93].

Secure Image steganography approach through two levels of security has suggested by AlWatyan et al. in first level, Character Bit Shuffler CBS is applied on this method to encrypt secure data .Then in second level, embed the encrypted data into image is done by Least Significant Bit LSB algorithm that is changed the last bits of the image pixels. This scheme has been tested with many images of size 100x100 and secret data size 1857 Bytes, which is automatically encrypted [94].

Panigrahy et al. have carried out the image steganography using secret key and the RGB channels of the cover image (JPEG). The idea of proposed method is to hide secret data into a deeper layer position of the selected RGB channel using secret key with modify the LSBs components for Blue and Green channels accordingly that causes minimum distortions [96].

Fouroozesh et al. have designed and analyzed the LSBMR algorithm for digital images steganography. They have also used sobel edge detection to find edges the true edge that can hide the secret data. The 200 images are used to conduct various experiments on this algorithm to improve the technique for the region identification. The gray-scale images is used in proposed method [97].

In order to enhance the security and minimize the distortion in image steganography algorithm based on AES encryption and reference data table RHT. In this work, a manner is used to structure reference data that is processed along with the stego-image to obtain the secret data and the AES encryption method is used to encrypt the reference data. The RHT is used to recorded the position of pixel value in the image, if the exists a pixel value in image which is same as the pixel value of secret image [98].

5- EVALUATION OF STEGANOGRAPHY

Four objectives and the Common evaluation that must be considered when creating a steganography method for measures the strengths and weaknesses points , as shown in Table 1.

Table 1 . Performance requirement

Parameters	requirement
Capacity	Must be High
Security	Must be High
Imperceptibility	Must be High
Computational Complexity	Must be low

1- **Capacity** . Refers to the Maximum amount of secret message which can be embedded into cover image without retraction of the image quality. It is usually represented in terms of bits per pixel.

2- Security. Security is one of the most important evaluation standard in steganography. A good steganographic technique should be resistance to steganalysis attacks.

3- Imperceptibility . Imperceptibility means the image transparency and quality for . After hiding secret message into cover image, Transparency and quality will be degraded into stego-image as compared to cover-image. So the result of stego image should be appears as possible as like the orignal image. the performance of stego image can be measured by peak signal-to-noise ratio (PSNR) which can be calculated by the difference distortion between the cover image and the stego image. PSNR is defined as:

$$PSNR = 10\ Log\ 10\left(\frac{C2_{max}}{MSE}\right)$$

Where MSE indicate to Mean Square Error that is defined as:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2$$

Where x and y are the coordinates of cover image, M and N are the dimensions of the cover image, (S_{xy}) is the generated stego-image and (C_{xy}) is the cover image.

4- Computational Complexity. How much costly and complexity computationally for embedding and extracting a hidden secret message.

This proposed reivew has describe carefully image steganography in spatial domain . Therefore, the frequency domain will not include in this reivew of image steganography.

6. CURRENT PROBLEMS, CHALLENGES AND OPEN RESEARCH ISSUES.

There are many works on the image steganography in spatial domain, Few of these work focusing on better image quality, while others aimed at payload capacity or provide more security method. The aim of those works is to get a robust method .In addition some of these works having impractical assumptions to secure the method, while the others can be used only for checking the effect of the method on different attacks.

According to the related work, the challenges and open issues in this important research is to accept the existence of the image steganography in spatial domain and dealing with this fact by detecting the weakness points and drawbacks during a new robust techniques. This open issue motivates the researchers to suggest an effective solution addressing this concern [107][108].

The summarization of the main characteristic features and the drawbacks of the image steganography techniques in spatial domain has been shown in Table 3. and Table 4. Respectively.

Table3: summarization of the main characteristic features

Ref	Capacity	Security	imperceptibility
9	Moderate	Moderate	High
13	Moderate	High	Moderate
16	Low	High	High
17	Moderate	High	Moderate
18	High	high	low
19	Low	High	High
20	High	Moderate	Low
21	Moderate	High	Moderate
22	Moderate	Moderate	Moderate
23	High	Moderate	Moderate
24	low	Moderate	High
26	low	High	High
27	high	High	low
28	Moderate	High	low
29	low	High	low
30	low	High	High
31	High	Moderate	low
32	low	Moderate	High
33	High	High	low
35	High	Moderate	Moderate
36	Moderate	high	Moderate
37	Low	high	high
38	Low	High	Moderate
39	High	Moderate	Low
41	High	High	Low
42	Moderate	Moderate	Low
43	High	High	Moderate
44	Moderate	High	Low
46	Low	High	Low
47	Moderate	Moderate	Moderate
48	Moderate	High	Low
49	Low	High	Moderate
50	High	Moderate	Low
51	Moderate	Moderate	Moderate
52	Low	High	High
53	Moderate	Moderate	Low
54	High	High	Low
55	Low	High	High
56	Moderate	High	Moderate
57	High	High	Moderate
58	Low	High	High
59	High	Moderate	Low
60	Moderate	High	Low
61	Moderate	Moderate	Low
62	Low	Moderate	Moderate
63	High	High	Moderate
64	High	High	Low
65	-	High	-
67	High	High	Low
68	High	Moderate	Low
69	High	High	Low
70	Moderate	High	Moderate

71	Low	High	high
72	High	Moderate	Low
73	Low	Moderate	Moderate
74	Low	Moderate	High
75	High	High	Low
76	High	High	Moderate
77	Moderate	High	-
78	Low	Moderate	-
79	Low	High	-
80	Moderate	Moderate	Low
81	-	High	Low
82	Low	Moderate	High
83	-	High	Moderate
84	High	Moderate	Moderate
85	Moderate	Moderate	-
86	High	Moderate	Moderate
87	Low	High	-
88	Moderate	Moderate	Moderate
89	High	High	-
90	Moderate	High	Low
91	Low	Moderate	Moderate
93	Moderate	Moderate	Low
94	Moderate	High	Moderate
96	Moderate	Moderate	Moderate
97	Moderate	Moderate	High
98	Moderate	High	Low

Table4: The Drawbacks of Image steganography Techniques in Spatial Domain.

Ref	Algorithms	Drawbacks
9	Edge detection and XOR coding	Imperceptibility.
13	LSB and genetic algorithm	Computationally Complex.
16	LSB	Works with color images only, Limitation in pixel selection (low capacity).
17	LSB and AT	Computationally Complex.
18	LSB and AT	Need the original image to extraction process, Computationally complexity because of different keys.
19	Edge detection and 2k correction	Capacity.
20	LSB Substitution	Original image is need in extraction process, security.
21	LSB and EMD	Computationally Complex.
22	BSS,RSA and LSB	Imperceptibility, robustness.
23	M-LSB and PBSA	Robustness.
24	Edge detection and LSBMR	Capacity, robustness.
26	NUBASI and AES	Capacity.
27	VLSB and VIVBS	Imperceptibility.
28	LSB and cryptograph	Imperceptibility, experimental Dataset is limited
29	Hash approach and edge detection	Imperceptibility, robustness, capacity.
30	LSB and AES	Computationally Complex.
31	PVD and DE	Imperceptibility, robustness.
32	LSB	Support color image only and experimental Dataset is limited.
33	GEMD	Imperceptibility.
35	Watermarking and LSB	Need original watermarked image for extraction process , robustness
36	Neural network, genetic algorithm and LSB	Robustness, Imperceptibility.
37	DKL	Computationally Complex.
38	LSB and NEQR	Computationally Complex, capacity.
39	MSB	High hidden capacity degrade the visual quality and Dataset is limited.
41	CLSM	Imperceptibility, robustness.
42	LSB	Experimental Dataset is limited.
43	Edge Detection and HSI	Experimental Dataset is limited and detected by statistical steganalysis.
44	LSB , Baker's map and Arnold cat map	Hidden capacity depended on Cover image pixel intensities, Imperceptibility.
46	LSB and ZDT	Algorithm is complex, capacity.
47	EG-LSB and canny Edge Detector	Limitation in pixels selection (low capacity), robustness.
48	LSB and PVD	Robustness.
49	LSB and Ken Ken Puzzle	Experimental Dataset is limited , Capacity
50	LSB and PVD	Imperceptibility , robustness
51	Block Entropy Segmentation	Robustness.
52	Vernam cipher and LSB	Limitation in pixels selection in cover image (Low capacity) and Experimental Dataset is limited.
53	Caesar‟s Cipher and LSB	Experimental Dataset is limited, robustness.
54	KBRP and GA	Experimental Dataset is limited and low Imperceptibility.
55	LSB	Robustness and low capacity
56	LSB and Data Mining	Experimental Dataset is limited and Limitation in pixels selection (low capacity).
57	4-bit LSB	Computationally Complex.
58	visual cryptography and LSB	Experimental Dataset is limited.
59	SLSB	Robustness.
60	LSB and GA	Experimental Dataset is limited, Imperceptibility.
61	Modified LSB	Experimental Dataset is limited, robustness.
62	RKDD	Robustness, capacity.
63	Multi-resolution images and LSB	Computationally Complex.
64	LSBs and 3-dimensional chaotic map	Computationally Complex and robustness.
65	Pseudo random matrix	Experimental Dataset is limited.
66	GA and histogram shifting	Imperceptibility, Computationally Complex.

67	Modified LSB	Robustness.
68	MHSBE and OPAP	Imperceptibility, Robustness.
69	ILSBMR	Imperceptibility.
70	TLEA, MS and LSB	Robustness, Computationally Complex.
71	SKA-LSB, TLEA and MLEA	Capacity.
72	Edge detection	Experimental Dataset is limited, Imperceptibility.
73	Dynamic programming	Robustness, Capacity.
74	sparse encoded matrix	Experimental Dataset is limited, robustness.
75	Chaotic Map and LSB	Imperceptibility, robustness.
76	AES and LSB	Imperceptibility.
77	OPAP and EBCDIC	Experimental Dataset is limited, robustness.
79	LSB	Experimental Dataset is limited, robustness.
80	AES and LSB	Imperceptibility, robustness.
81	Neural network and edge detection	Imperceptibility, Experimental Dataset is limited.
82	standard LSB and Condition LSB	Capacity, robustness.
83	DES and LSB	Robustness.
84	LSB	Robustness.
85	AMBTC	Computationally Complex.
86	8 scanning orders and LSB	Imperceptibility, experimental Dataset is limited.
87	standard LSB	Capacity, experimental Dataset is limited.
88	LSB and edge adaptive	Robustness.
89	Mottling through Morphing and LSBs	Robustness, experimental Dataset is limited.
90	Chaos theory and LSB	Imperceptibility
91	LSB and primitive root numbers	Experimental Dataset is limited.
93	tri-pixel unit and 2LSB	Imperceptibility, robustness.
94	LSB and FPGA Implementation	Imperceptibility, Computationally Complex.
96	LSBs	Imperceptibility, robustness.
97	LSBMR and sobel edge detection	Robustness.
98	Closest pixel-pair mapping and AES	Imperceptibility, robustness.

7. CONCLUSION

Information hiding is becoming an extensive field that fetch a serious research interest. This is the reason steganography is earning more attraction to secure data though network communication. This study summarizes the current image steganography techniques in spatial domain, also analyzed different problems and the drawbacks of each method that have been innovated from last few years. Every technique differs from every other technique. Few of them work on better image quality, while others works on data hiding capacity or security. All these techniques can be give more efforts and vital for future research in steganography. Finally, the open issues of this work motivates the researchers to suggest an effective solution addressing this concern.

REFRENCES:

[1] Laurel, Carlos Ortega, Shi-Hai Dong, and M. Cruz-Irisson. "Steganography on quantum pixel images using Shannon entropy." *International Journal of Quantum information* 14.05 (2016): 1650021.

[2] 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.

[3] Ghebleh, M., and A. Kanso. "A robust chaotic algorithm for digital image steganography." *Communications in Nonlinear Science and Numerical Simulation* 19.6 (2014): 1898-1907.

[4] 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.

[5] Zhang, Lingyu, and Hongwei Li. "A product code in steganography with improved embedding rate." *Information Technology, Networking, Electronic and Automation Control Conference, IEEE. IEEE, 2016.*

[6] Al-Omari, Zaid, and Ahmad T. Al-Taani. "A Survey on Digital Image Steganography."

[7] Banerjee, Indradip, Souvik Bhattacharyya, and Gautam Sanyal. "Robust image steganography with pixel factor mapping (PFM) technique." *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*. IEEE, 2014.

[8] Lwin, Thandar, and PHYO SUWAI. "Information Hiding System Using Text and Image Steganography." *International Journal of Scientific Engineering and Technology Research* 3.4 (2014): 1972-1977.

[9] Al-Dmour, Hayat, and Ahmed Al-Ani. "A steganography embedding method based on edge identification and XOR coding." *Expert systems with Applications* 46 (2016): 293-306.

[10] Dimitrova, Biljana, and Aleksandra Mileva. "Steganography of Hypertext Transfer

Protocol Version 2 (HTTP/2)." *Journal of Computer and Communications* 5 (2017): 98-111.

[11] Dagar, Ekta, and Sunny Dagar. "LSB based image steganography using x-box mapping." *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014.

[12] Singla, Deepali, and Mamta Juneja. "An analysis of edge based image steganography techniques in spatial domain." *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*. IEEE, 2014.

[13] Kanan, Hamidreza Rashidy, and Bahram Nazeri. "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 (2014): 6123-6130.

[14] Tiwari, Anjali, Seema Rani Yadav, and N. K. Mittal. "A review on different image steganography techniques." *International Journal of Engineering and Innovative Technology (IJEIT) Volume* 3 (2014): 19-23.

[15] Wu, Kaicheng. "Research of Spread Spectrum Steganography based on High-order Markov Model." *DEStech Transactions on Computer Science and Engineering* iccae (2016).

[16] Al-Tamimi, Abdul-Gabbar Tarish, and Abdulmalek Abduljabbar Alqobaty. "Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm." *International Journal of Computer Science and Information Security* 13.1 (2015): 1.

[17] Das, Sujit Kumar, and Bibhas Chandra Dhara. "An Image Secret Sharing Technique with Block Based Image Coding." *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*. IEEE, 2015.

[18] Das, Pallavi, Satish Chandra Kushwaha, and Madhuparna Chakraborty. "Multiple embedding secret key image steganography using LSB substitution and Arnold transform." *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on*. IEEE, 2015.

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

[20] Mohamed, Marghny H., and Loay M. Mohamed. "High Capacity Image Steganography Technique based on LSB Substitution Method." *Applied Mathematics & Information Sciences* 10.1 (2016): 259.

[21] Kuo, Wen-Chung, Chun-Cheng Wang, and Hong-Ching Hou. "Signed digit data hiding scheme." *Information Processing Letters* 116.2 (2016): 183-191.

[22] Nayak, Rakesh. "Steganography with BSS-RSA-LSB technique: A new approach to Steganography." *IJSEAT* 3.5 (2015): 187-190.

[23] Muhammad, Khan, et al. "A new image steganographic technique using pattern based bits shuffling and magic LSB for grayscale images." *arXiv preprint arXiv:1601.01386* (2016).

[24] Mungmode, Sachin, R. R. Sedamkar, and Niranjan Kulkarni. "An Enhanced Edge Adaptive Steganography Approach using Threshold Value for Region Selection." *arXiv preprint arXiv:1601.02076* (2016).

[25] Zhang, Hao, Tao Zhang, and Huajin Chen. "Variance Analysis of Pixel-Value Differencing Steganography." *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*. ACM, 2017.

[26] 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.

[27] Khan, Sahib, Nasir Ahmad, and Muneeza Wahid. "Varying index varying bits substitution algorithm for the implementation of VLSB steganography." *Journal of the Chinese Institute of Engineers* 39.1 (2016): 101-109.

[28] Thakur, Priyanka, Santosh Kushwaha, and Yogesh Rai. "Enhance Steganography Techniques: A Solution for Image Security." *International Journal of Computer Applications* 115.3 (2015).

[29] Singh, Saurabh, and Ashutosh Datar. "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 (2015): 92.

[30] Patel, Farah R., and A. N. Cheeran. "Performance Evaluation of Steganography and AES encryption based on different formats of the Image." *Performance Evaluation* 4.5 (2015).

[31] Jana, Biswapati, Debasis Giri, and Shyamal Kumar Mondal. "Dual-Image Based

Reversible Data Hiding Scheme Using Pixel Value Difference Expansion." *IJ Network Security* 18.4 (2016): 633-643.

[32] Al-Tamimi, Abdul-Gabbar Tarish, and Abdulmalek Abduljabbar Alqobaty. "Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm." *International Journal of Computer Science and Information Security* 13.1 (2015): 1.

[33] Kuo, Wen-Chung, et al. "Secure multi-group data hiding based on gemd map." *Multimedia Tools and Applications* 76.2 (2017): 1901-1919.

[34] Das, Pallavi, Satish Chandra Kushwaha, and Madhuparna Chakraborty. "Multiple embedding secret key image steganography using LSB substitution and Arnold transform." *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on*. IEEE, 2015.

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

[36] 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.

[37] Udhayavene, S., Aathira T. Dev, and K. Chandrasekaran. "New data hiding technique in encrypted image: DKL algorithm (differing key length)." *Procedia Computer Science* 54 (2015): 790-798.

[38] Jiang, Nan, Na Zhao, and Luo Wang. "LSB based quantum image steganography algorithm." *International Journal of Theoretical Physics* 55.1 (2016): 107-123.

[39] Patil, Venkat P., Umakant Bhaskar Gohatre, and R. B. Sonawane. "An Enhancing PSNR, Payload Capacity and Security of Image using Bits Difference Base on Most Significant Bit Techniques." *International Journal of Advanced Electronics and Communication Systems* 6.2 (2017).

[41] Kocak, Cemal. "CLSM: COUPLE LAYERED SECURITY MODEL A HIGH-CAPACITY DATA HIDING SCHEME USING WITH STEGANOGRAPHY." *Image Analysis & Stereology* 36.1 (2017): 15-23.

[42] Sharifzadeh, Mehdi, et al. "A New Parallel Message-distribution Technique for Cost-based Steganography." *arXiv preprint arXiv:1705.08616* (2017).

[43] Yadav, Vandana, and Sanjay Kumar Sharma. "A New Approach for Image Steganography Using Edge Detection Method for Hiding Text in Color Images Using HSI Color Model." (2017).

[44] BUKHARI, S., et al. "Chaos Image Encryption Followed By the Steganography Technique." *Sindh University Research Journal-SURJ (Science Series)* 49.1 (2017).

[45] Al-Omari, Zaid Y., and Ahmad T. Al-Taani. "Secure LSB steganography for colored images using character-color mapping." *Information and Communication Systems (ICICS), 2017 8th International Conference on*. IEEE, 2017.

[45] Al-Omari, Zaid Y., and Ahmad T. Al-Taani. "Secure LSB steganography for colored images using character-color mapping." *Information and Communication Systems (ICICS), 2017 8th International Conference on*. IEEE, 2017.

[46] Sharma, Shivani, Virendra Kumar Yadav, and Saumya Batham. "Zero Distortion Technique: An Approach to Image Steganography Using Strength of Indexed Based Chaotic Sequence." *International Symposium on Security in Computing and Communication*. Springer, Berlin, Heidelberg, 2014.

[47] Chaturvedi, Krishna Nand, and Amit Doeger. "A Novel Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images." *International Journal of Computer Applications* 86.7 (2014).

[48] Gulve, Avinash K., and Madhuri S. Joshi. "An image steganography algorithm with five pixel pair differencing and gray code conversion." *International Journal of Image, Graphics and Signal Processing* 6.3 (2014): 12.

[49] Vidya, G., et al. "Image steganography using ken ken puzzle for secure data hiding." *Indian Journal of Science and Technology* 7.9 (2014): 1403-1413.

[50] Swain, Gandharba. "Digital image steganography using nine-pixel differencing and modified LSB substitution." *Indian Journal of Science and Technology* 7.9 (2014): 1444-1450.

[51] Roy, Ratnakirti, and Suvamoy Changder. "Image steganography with block entropy based segmentation and variable rate embedding." *Business and Information Management (ICBIM), 2014 2nd International Conference on*. IEEE, 2014.

[52] Thomas, Ajin P., et al. "Secret Data Transmission Using Combination of Cryptography &Steganography." *International Journal* 4.5 (2017): 171-175.

[53] Rahate, Nikhil D., and P. R. Rothe. "Data Hiding Technique for Security by using Image Steganography." *International Conference on Industrial Automation and Computing*. 2014.

[54] Soumi, C. G., Joona George, and Janahanlal Stephen. "Genetic algorithm based mosaic image steganography for enhanced security." *International Journal on Signal and Image Processing* 5.1 (2014): 15.

[55] Umamaheswari, G., and C. P. Sumathi. "A New Information Hiding Technique Matching Secret Message And Cover Image Binary Value." *International Journal of Computer Science and Information Security* 15.1 (2017): 321.

[56] Devadiga, Namrata, et al. "E-Banking Security using Cryptography, Steganography and Data Mining." *International Journal of Computer Applications* 164.9 (2017).

[57] Thakre, Ketki, and Nehal Chitaliya. "Dual Image Steganography for Communicating High Security Information." *International Journal of Soft Computing and Engineering (IJSCE)* 4.3 (2014).

[58] Rajendran, Reshma, and Amrutha V. Nair. "Secure Communication in Online Payment." *International Journal of Engineering Science* 11457 (2017).

[59] Klim, Sahar Mahdie. "SELECTED LEAST SIGNIFICANT BIT APPROACH FOR HIDING INFORMATION INSIDE COLOR IMAGE STEGANOGRAPHY BY USING MAGIC SQUARE." *Journal of Engineering and Sustainable Development Vol* 21.01 (2017).

[60] Gaidhani, Chaitali R., Vedashree M. Deshpande, and Vrushali N. Bora. "Image Steganography for Message Hiding Using Genetic Algorithm." *International Journal of Computer Sciences and Engineering* 2.3 (2014): 67-70.

[61] Nimje, Swati, et al. "Hiding existence of communication using image steganography." *International Journal of Computer Science and Engineering* 2 (2014): 163-166.

[62] Alsarayreh, Maher A., Mohammad A. Alia, and Khulood Abu Maria. "A NOVEL IMAGE STEGANOGRAPHIC SYSTEM BASED ON EXACT MATCHING ALGORITHM AND KEY-DEPENDENT DATA TECHNIQUE." *Journal of Theoretical and Applied Information Technology* 95.5 (2017): 1212.

[63] Hosam, Osama, and Zohair Malki. "Steganography technique for embedding secure data into the image regions with abrupt changes." *Life Sci J* 11.9 (2014): 126-130.

[64] Sharif, Ami, Majid Mollaeefar, and Mahboubeh Nazari. "A novel method for digital image steganography based on a new three-dimensional chaotic map." *Multimedia Tools and Applications* 76.6 (2017): 7849-7867.

[65] Mocanu, Stefan, et al. "Improved Security Based on Combined Encryption and Steganography Techniques." *Studies in Informatics and Control* 26.1 (2017): 115-126.

[66] Wang, Junxiang, et al. "Rate and distortion optimization for reversible data hiding using multiple histogram shifting." *IEEE transactions on cybernetics* 47.2 (2017): 315-326.

[67] Rashid, M. Khurrum Rahim, Saad Missen, and Aqsa Rashid. "Robust Increased Capacity Image Steganographic Scheme." *Transformation* 5.11 (2014).

[68] Gupta, Piyush Kumar, Ratnakirti Roy, and Suvamoy Changder. "A secure image steganography technique with moderately higher significant bit embedding." *Computer Communication and Informatics (ICCCI), 2014 International Conference on*. IEEE, 2014.

[69] Nikseresht, Sajad, Mashallah Abbasi Dezfouli, and Seyed Enayatallah Alavi. "ILSBMR: improved LSBMR (ILSBMR) method." *Multimedia Tools and Applications* 76.2 (2017): 1857-1874.

[70] Muhammad, Khan, et al. "Image steganography for authenticity of visual contents in social networks." *Multimedia Tools and Applications* (2017): 1-20.

[71] 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.

[72] Islam, Saiful, Mangat R. Modi, and Phalguni Gupta. "Edge-based image steganography." *EURASIP Journal on Information Security* 2014.1 (2014): 8.

[73] Baghel, Anshu, and Mrs Suchitra Pandey. "Data Hiding in Images using Dynamic Programming considering Human Visual System." (2017).

[74] Shah, Vipul. "Sparse Encoded Matrix based Steganography algorithm." (2017).

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

[76] Juneja, Mamta, and Parvinder Singh Sandhu. "Improved LSB based Steganography Techniques for Color Images in Spatial Domain." *IJ Network Security* 16.6 (2014): 452-462.

[77] Karthikeyan, B., et al. "An Improved Steganographic Technique Using LSB Replacement on a Scanned Path Image." *IJ Network Security* 16.1 (2014): 14-18.

[78] Sehgal, Nancy, and Ajay Goel. "Evolution in Image Steganography." *International Journal of Information & Computation Technology* 4 (2014): 1221-1227.

[79] Bansod, Sneha, and Gunjan Bhure. "Data encryption by image steganography." *Int. J. Inform. Comput. Technol. Int. Res. Publ. House* 4 (2014): 453-458.

[80] Suryawanshi, Divya, Meetali Salvi, and Soumya Pandey3z. "Image steganography for criminal cases." (2017).

[81] Khan, Imran. "An Efficient Neural Network based Algorithm of Steganography for image." *International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume* 1 (2014): 63-67.

[82] Manaseer, Saher, Asmaa Aljawawdeh, and Dua Alsoudi. "A New Image Steganography Depending On Reference & LSB." *International Journal of Applied Engineering Research* 12.9 (2017): 1950-1955.

[83] Ren-Er, Yang, et al. "Image steganography combined with DES encryption pre-processing." *Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on*. IEEE, 2014.

[84] Akhtar, Nadeem, Shahbaaz Khan, and Pragati Johri. "An improved inverted LSB image steganography." *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*. IEEE, 2014.

[85] Huang, Ying-Hsuan, Ching-Chun Chang, and Yi-Hui Chen. "Hybrid secret hiding schemes based on absolute moment block truncation coding." *Multimedia Tools and Applications* 76.5 (2017): 6159-6174.

[86] AYDOĞAN, TURGAY, and CÜNEYT BAYILMIŞ. "A new efficient block matching data hiding method based on scanning order selection in medical images." *Turkish Journal of Electrical Engineering & Computer Sciences* 25.1 (2017): 461-473.

[87] Rura, Lauretha, Biju Issac, and Manas Kumar Haldar. "Online Voting System Based on Image Steganography and Visual Cryptography." *Journal of computing and information technology* 25.1 (2017): 47-61.

[88] 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.

[89] Bajpai, Sanjay, and Kanak Saxena. "A High End Capacity in Digital Image Steganography: Empowering Security by Mottling through Morphing." *Proceedings of the 2014 International Conference on Communications, Signal Processing and Computers*. 2014.

[90] Bandyopadhyay, Debiprasad, et al. "A novel secure image steganography method based on Chaos theory in spatial domain." *International Journal of Security, Privacy and Trust Management (IJSPTM)* 3.1 (2014): 11-22.

[91] Al-Saiyd, Nedhal AM. "Hybrid Medical Colored Image LSB Steganography Based on Primitive Root Numbers." *International Journal of Computer Science and Network Security (IJCSNS)* 17.2 (2017): 206.

[92] Hajduk, Vladimír, and Dušan Levický. "Accelerated cover selection steganography." *Radioelektronika (RADIOELEKTRONIKA), 2017 27th International Conference*. IEEE, 2017.

[93] Yu, Xiangyu, et al. "An adaptive tri-pixel unit steganographic algorithm using the least two significant bits." *Biometrics and Forensics (IWBF), 2017 5th International Workshop on*. IEEE, 2017.

[94] AlWatyan, Abdullah, et al. "Security approach for LSB steganography based FPGA implementation." *Modeling, Simulation, and Applied Optimization (ICMSAO), 2017 7th International Conference on*. IEEE, 2017.

[95] Sonawane, Rashmi A., and Mrs Dipti Sonawane. "Reversible Texture Synthesis Using Three Level Security in Steganography." (2017).

[96] Bairagi, Anupam Kumar, Saikat Mondal, and Rameswar Debnath. "A robust RGB channel based image steganography technique using a secret key." *Computer and Information Technology (ICCIT), 2014 16th.*

[97] Fouroozesh, Zohreh, and Jihad Al ja'am. "Image steganography based on LSBMR using sobel edge detection." *e-Technologies and Networks for Development (ICeND), 2014 Third International Conference on*. IEEE, 2014.

[98] 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.

[99] Araghi, Tanya Koohpayeh, et al. "A survey on digital image watermarking techniques in spatial and transform domains." *Int. J. Adv. Image Process. Techn.–IJIPT* 3.1 (2016): 6-10.

[100] Bhattacharyya, S., Khan, A., Nandi, A., Dasmalakar, A., Roy, S., & Sanyal, G. (2011, December). Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography. In *Information and Communication Technologies (WICT),IEE, 2011 World Congress on* (pp. 36-41).

[101] Motameni, H., et al. "Labeling method in Steganography." *Proceedings of world academy of science, engineering and technology*. Vol. 24. 2007.

[102] Fridrich, Jiri. "A new steganographic method for palette-based images." *PICS*. 1999.

[103] 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.

[104] 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).

[105] MAHMOOD, ALI SHAKIR, MOHD RAHIM, and MOHD SHAFRY. "GENERATING AND EXPANDING OF AN ENCRYPTION KEY BASED ON KNIGHT TOUR PROBLEM." *Journal of Theoretical & Applied Information Technology* 95.7 (2017).

[106] Harouni, M., et al. "Online Persian/Arabic script classification without contextual information." *The Imaging Science Journal* 62.8 (2014): 437-448.

[107] SaberiKamarposhti, Morteza, et al. "Using 3-cell chaotic map for image encryption based on biological operations." *Nonlinear Dynamics* 75.3 (2014): 407-416.

[108] MAHMOOD, ALI SHAKIR, MOHD RAHIM, and MOHD SHAFRY. "GENERATING AND EXPANDING OF AN ENCRYPTION KEY BASED ON KNIGHT TOUR PROBLEM." *Journal of Theoretical & Applied Information Technology* 95.7 (2017).

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

[110] Nagpal, Kirti D., and D. S. Dabhade. "A Survey on Image Steganography & its Techniques in Spatial & Frequency Domain."

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