International Journal of Engineering & Technology, 7 (4) (2018) 3505-3514

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.17294
Research paper

Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats

Mohammed Mahdi Hashim [1, 3] *, Mohd Shafry Mohd Rahim [1, 2], Fadil Abass Johi [5], Mustafa Sabah Taha [1, 4], Hassan Salman Hamad [6]

[1] *School of Computing, Facility of Engineering, University Technology Malaysia, Johor Bahru, Malaysia*
[2] *UTM (IRDA) Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia*
[3] *Faculty of Engineering, Uruk University, Baghdad, Iraq*
[4] *Basrah Oil Training Institute ,Ministry of Oil, Iraq*
[5] *Missan Oil Company ,Ministry of Oil, Iraq*
[6] *Middle Technical University, Technical Instructors Training Institute, Baghdad, Iraq*
**Corresponding author E-mail: comp.mmh@gmail.com*

Abstract

Recently, Steganography is an outstanding research area which used for data protection from unauthorized access. Steganography is defined as the art and science of covert information in plain sight in various media sources such as text, images, audio, video, network channel etc. so, as to not stimulate any suspicion; while steganalysis is the science of attacking the steganographic system to reveal the secret message. This research clarifies the diverse showing the evaluation factors based on image steganographic algorithms. The effectiveness of a ste-ganographic is rated to three main parameters, payload capacity, image quality measure and security measure. This study is focused on im-age steganographic which is most popular in in steganographic branches. Generally, the Least significant bit is major efficient approach utilized to embed the secret message. In addition, this paper has more detail knowledge based on Least significant bit LSB within various Images formats. All metrics are illustrated in this study with arithmetical equations while some important trends are discussed also at the end of the paper.

Keywords: *Image Steganography; Least Significant Bit (LSB); Steganalysis; Image Histogram; Image Quality Measurement.*

1. Introduction

Steganography is an important branch of information hiding, where secret contents are concealment in carrier file like image for concealing its presence without a distortion in a carrier. Fundamentally, steganography mechanisms have six types: image steganography, audio steganography, video steganography, text steganography, DNA steganography and protocol steganography as presentational in Fig.1. Steganography is provider a powerful security, especial when it is jointed with digital images due the it has different formats which can be applied. Image steganography can be hiding the unnatural secret message within a carrier image, so the carrier image quality will have a small change, thus no one cannot recognize it [2]. Image steganography techniques are classified in two prime kinds, spatial domain and frequency domain (transform) [1].

the mechanism of spatial domain implement procedure directly into the all pixels of carrier image while embedding the secret message to frequency domain will done after several conversions to convert the image to frequency domain. The stego image name comes from the concealed secret message within image. Many methods are belonged into spatial domain such as, LSB (matching and substitution), Gray level modification GLV, etc, [20]. The frequency domain methods are utilizing different converts such as Discrete cosine transform DCT, Discrete Fourier Transform DFT, etc [1]. Another mechanism is done within steganographic which called reversible steganographic. This mechanism is work by recover the carrier image along to the secret information from the stego image [3]

The least significant bit LSB substitution is the most popular into image steganography techniques. The LSB substitution can be suitable extensive up to 4 LSB planes to obtained higher payload capacity while it is easy to execute. It is vulnerable to several attack like RS analysis [4]. In order to solve this issue, the LSB can used in the different manner. LSB array can generated by using all the LSB bits within pixels. The secret message in binary format can be concealed at less deformation position of LSB bits array to improve the security [5].

The three of LSB bits can checked to enhance the payload capacity with high security where only two bits can be used to hidden within two random chosen bits depending on the secret message, this is named as data dependent embedding [6,7,8]. Evaluation Factors of image steganography has fundamental importance to numerous image processing applications and evaluate the methods. The quality of images could less degrade in the point which used to hide secret message, it can be see that by a Human eye. Automatically algorithms are used for image quality estimate that could analyze it and report their quality with payload capacity and security, so this is the objective of evaluation.

Many review papers have been published on statistics evaluation which is able to use to distinguish between carrier image and stego

Copyright © 2018 Mohammed Mahdi Hashim et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

images that obtained through different embedding techniques [9 - 11]. though former works observe sensible success on controlled data sets, there is a shortage of estimate on how various suggested techniques compare to each other. This is mainly due former work is limited either by the number of embedding techniques or the quality of the data set used to the classification technique used.
The main contribution in our research is to clarify the details of different evaluation parameters to obtain the high performance of image steganography. in additional, this paper also presents elaborate knowledge on the LSB based image steganography in different Images formats.

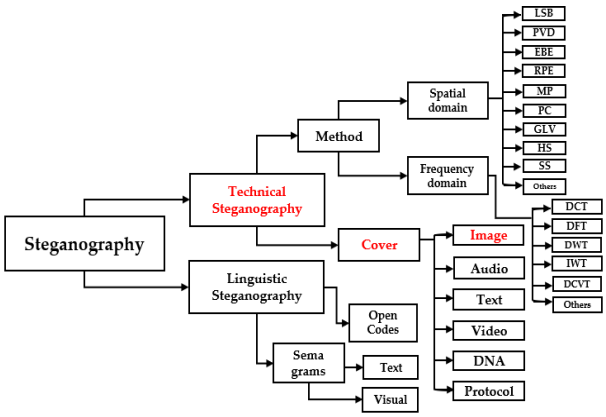


Fig. 1: Taxonomy of Steganography.

The rest of the research is ordered as follows. In section 2, the problem definition of steganography was discussed while an overview of image steganography is presented in section 3. In section 4, image analysis has been described in detail. In section 5, the LSB technique with various embedding bits was characterized. The different evaluation parameters are given in section 6. In section 7, evaluate some different image format is noticed while section 8 feature direction was discussed. Finally, the conclusion of the paper was given.

2. Problem definition of steganography

The thought of steganography framework has been introduced by Simmons in 1984 [12], with the example of prisoner's secret message. The escape plan for Alice and Bob who wishes to communicate inside the prison where all the communication and messages must go through the warden. Wendy who at the slightest suspicion of secret information will put them in solitary imprisonment. The idea of steganography is generally modeled by prisoner's issue as showed in figure 2. Alice hides the secret message "M" into a cover-image "C" using an optional key which represent as 'K'. this operation a will generate the stego image "S", which is sent over a public channel. Consequently, the data embedding procedure can be indicated as below:

Embedding scheme: $C \times M \times k \rightarrow S$, $s = Emb(x,m,k)$

Extraction scheme: $C \times k \rightarrow M$, $m = Ext\ (s, k)$.

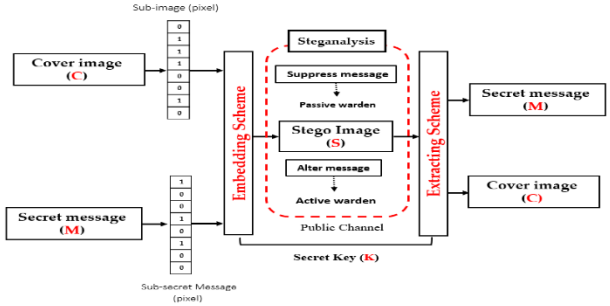


Fig. 2: Illustrate Steganography Process.

Consequently, according to Figure 2, we have the following definitions:
Cover-image (C): also called the carrier image, it utilized as the medium to conceal the secret data using some embedding algorithms. Stego image (S): It is the result gained after embedding the secret message (k) which is an aim of image steganography system. the stego image must be the same quality as the cover image without distorting the cover image quality. Secret Key (K): used to encode /decode the hidden message. Secret Message (M): Can be anything like data, file or image etc, that can hide within cover image. Wendy could be either passive or active rely on the kind of action she carries out on suspicion. A passive warden would simply suppress or ignore while an active warden would alter the message to foil the escape plan. We suppose in our study that Wendy is a passive warden and cannot distinguish between cover image and stego image. Therefore, steganalysis is the technique that assistances wendy in extricating the secret message from the stego image. She analyses the embedding distortions and other statistical artifacts introduced in the image post embedding to derive at the technique to break the steganographic method. It can be rightly pointed that development of steganography and steganalysis go parallel.

3. Image steganography

Steganography has recently become an important image working tool due to the inability of the human eye to focus on the sensitive details of photos. A little change in the steganography of an image has no tangible effect on the image. The selection of an image with masked information is important in the design of steganography systems, while bottom colors uniform textured images are not suitable for steganography. Image steganography comes in various techniques and their major target is to have access to high capacity, security, and robustness.
There are several steganography compression techniques, but only two types (lossy compression and lossless compression) are used in image steganography. Example of lossless compression formats is a Huffman coding which offers more pledges [13]. Almost all data hiding techniques aim at the modification of insignificant data in the cover image. One of the commonest methods of concealing secret cover image information is the least significant bit (LSB) injection approach. Most of the simple schemes have suggested the placement of the embedding data at the LSB of each cover image pixel [14], [15]. A modification of the LSB has no significant influence on the image quality from the human perspective, but it is more sensitive to several statistical attacks, including cropping and compression. The secret messages can be hidden by using the moderate significant bits in the cover image's pixel. The length of the LSB secret messages has been experimentally proven to be predestined with comparatively high precision.

4. Image analysis

A computer image represents a collection of numbers which shape several light densities in different image regions. These numbers give rise to a grid and each point is indicated as a pixel. Internet images consist of rectangular pixel maps (pixels are depicted as bits) and each pixel has a specified color and location. These pixels are horizontally presented row-wise. In each color scheme, the bits are referred to as the bit depth which signifies the number of bits used per pixel (where 8 is the least bit depth in the current color schemes). This implies that 8 bits are used to characterize each pixels' color. For the grayscale images, each pixel comprises of 8 bits and can characterize 256 different shades of grey colors. For digital color images (also known as true color), the RGB color model uses 24 bits [16]. In a 24-bit image, all the color variations are sourced red, green, and blue (RGB) and each color are performed by 8 bits. However, each pixel can comprise of 256 various amounts of RGB, summing up to >16 million combinations and > 16 million colors [18].

5. The LSB approach

The 8th bit of the LSB in an image can be changed to a secret message bit. With the RGB pixel in an image (24-bits), 3 bits can be stored within each pixel by altering a bit each of RGB components as they are each represented by a byte. An image of 800 × 600 pixel size can store a total of 180,000 bytes or 1,440,000 bits of secret embedded messages. The LSB part of the carrier image is utilized to embed an information. Figure 3 is a simple example of hiding the number 300 into the first 8 bytes, where only 5 bits are required to be altered in the embedded secret information [19]. Therefore, embedding a secret message with the maximum carrier size requires altering only half of the image bits. Each primary color consists of about 256 potential intensities. There are small variations in the intensity of the colors when the LSB is changed. The human eye cannot comprehend these changes due to its insensitivity to color progression; so, the secret message is successfully embedded [18].

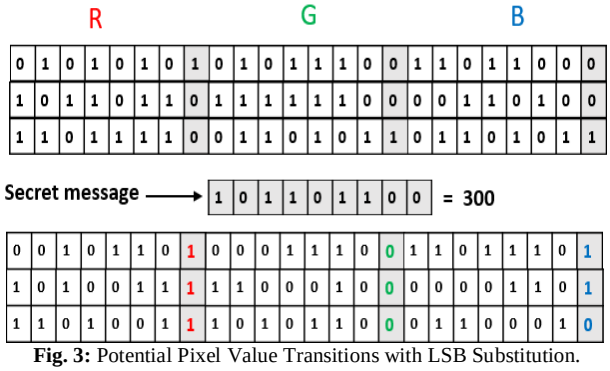


Fig. 3: Potential Pixel Value Transitions with LSB Substitution.

5.1. Least significant bit (LSB) in BMP

The BMP is also known as bitmap image file; it is not exceedingly applied with steganography as a carrier image due to more suspicious tendencies when transferring the secret message in the LSB stego. The application of BMP image in steganography as the carrier is always followed by the alteration of one or more of the bytes that make up the image pixel. The secret message can be stored within the LSB of one color of the RGB (24 bits) value or at the valence bit of the complete RGB value. A large message can be concealed quite within a BMP image. The LSB in BMP is must suitable for implementations where the focus is in the payload capacity of data to be transferred and not on a secret of that data. A change in the number of bits can improve the possibility of noticing the altered bits by the human eye. The major aim of steganography is to transmit a secret message to an intended destination without any intrusion [20-21].

Stego image with 1- LSB, in this method, a single LSB bit in the carrier image is changed, and such change only results in a change in the bytes' integer value by [1]; hence, this change is insignificant. The change of a more significant bit can result in a proportional alteration in the visible color appearance. The LSB of one of the colors accounts for the pixels' RGB value. Thus, this must have a minimal influence on the appearance of the carrier image. The aforementioned procedure gives rise to new colors for the palette. When a carrier image has a palette size of 128 pixels, there is a need to create a new color for each color present in the palette. Therefore, the application of a 128-palette image can result in a significant distortion of the original image [22].

Stego image with 2- LSB, in this method, about twice as much information can be stored. It is an improvement of the previous method because, in this method, [2] LSBs in each color within the RGB value of the pixels is used to store the bits of the secret message in the carrier image. The palette of the carrier image will still contain 68 colors; thus, the storage of the stego data involves 2 bits. There should be a maximum of 64 colors in the palette, i.e. there must be [3] new colors for each color present. There will be fewer colors for the starting image demonstration, hence, will be more decadent compared to the image used in the stego one-bit method. Thus, the LSB of [2] colors in the RGB value could have been utilized in this method and that would have conferred the same storage size [23].

Stego image with 3- LSB, this method has a higher data hiding capacity as its storage capacity is about 3 times that of stego one bit. The use of 128-color palette in this method results in more image distortion. This method stores message bits using 3 LSBs of each color in the RGB pixel value. This will result in a combination of 3 new colors for each existing color (making up 224 new colors), leading to the use of a palette with a maximum of 32 colors only.

Stego image with 4- LSB, this method has a data hiding capacity of about 4 times that of stego one bit. The use of 128-color palette in this method also results in image distortion. This method uses 4 LSBs of each color in the RGB pixel value for message bits storage. It involves the use of a palette of 16 colors which will result in a combination of [3] new colors per color (giving 240 new colors) and requires the involvement of a palette with a maximum of 32 colors only. Changing [4] LSB bits of each of red green and blue pixels may result in some amount of texture change.

5.2. Least significant bit (LSB) in GIF

The suspicion that usually accompanies the use of PNG may not arise if coupled within an LSB stego image. The images can be utilized as a carrier in steganography, which are generally altered by changing some of the bits or bytes that make up the image pixels. Such secret message can store in the LSB of one RGB color pixel value, or in corresponding bit of the whole RGB color value. The PNG can hide several messages, LSB in PNG is most suitable for applications which focus on the volume of information to be disseminated rather than on the secret detail of the information. The alteration of more or more number of bits can result in a higher chance of noticing the altered bits with the human eye. With LSB, steganography mainly aims at the dissemination of a message without any form of intrusion [24-25].

5.3. Least significant bit (LSB) in PNG

As we know, the Graphics Interchange Format (GIF) has only eight (8) bits depth, so, the information hiding capacity is lower compared to BMP. The hiding of information using LSB has the same result in both GIF and BMP. The LSB approach is considered as most effective for embedding a reasonable capacity of information. In the GIF image, the colors used are stored in a palette because it is an indexed image. Each pixel is represented as a byte and the pixel data is considered as color palette index. The commonly used color is ordered from the palette to the least used colors to reduce lookup time. The use of a GIF image as a carrier for steganographic requires some levels of carefulness because of the issue with the palette scheme. The use of a GIF image with an altered LSB as a palette scheme may give different colors due to the change in the color palette index. Whenever there are different neighboring palette entries, there is a remarkable image change, but when there is a similar neighboring palette entry, the change is not remarkable [26]. Generality, applications that deploy LSB approaches on GIF image are characterized with low security due to the possibility of detecting even an average change in the image. Such issues can be solved thus:

i) The palette must be isolated if there is a reduced difference between sequential colors.
ii) New colors which visually resemble the colors currently in the palette must be added.
iii) An 8-bit grayscale GIF image comprising of 256 gray shades must be used; else, there will be a gradual alteration of the colors.

6. Evaluation of image steganography

Three objectives must be considered when creating any steganography method (Security, Capacity and Image quality) as we mention in section 3. Generally, figure 4 is showed the details of evaluation parameters. In order to evaluation and measures these objectives to obtain the strengths and weaknesses points of the system, we can use the following measurements:

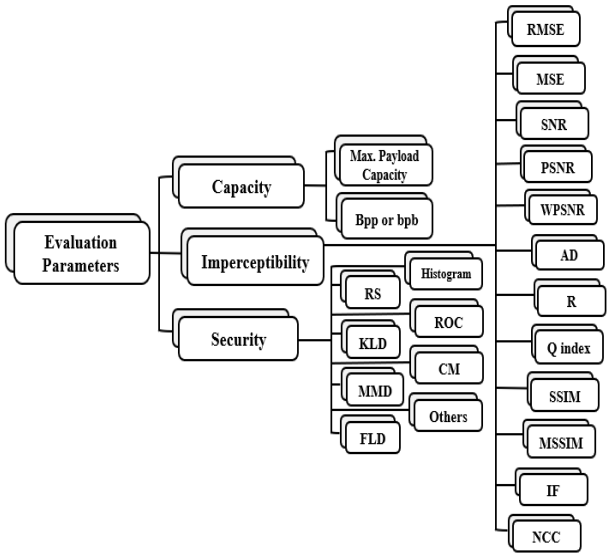


Fig. 4: Evaluation Parameters.

6.1. Payload capacity measurement

The capacity is indicated as a maximum payload capacity and bit rate as shown in Figure 3. Payload capacity refers to the number of embeddable secret bits; ideally, the capacity of the algorithm should be as high as possible while ensuring that the stego image quality is acceptable without any significant visual or statistical distortion. Several studies have clarified payload capacity in a different way (such as bits, bytes, and even kilobytes), but often, it is described as either bit per pixel (bpp) or bits per byte (bpb). The bit rate is referred to a large number of bits that can be concealed within a pixel for spatial or bits per transform coefficient transform [27,28].

6.2. Security measurement

One of the important evaluation parameters to be considered during the design of any application is its security or undetectability. Steganographic systems are susceptible to several types of stego attacks which may allow an eavesdropper to have access to the secret message bits embedded in a cover media. Stego attackers often concentrate on the retrieval or detection of the presence of secret data bits from a stego-image [29]. Figure 4 presents a detailed discussion of different steganalysis methods.

6.2.1. Regular and singular (RS)

Regular and Singular (RS) analysis has been proposed for the detection of random LSB embedding methods [38]. It is commonly used to check for the resistance of steganographic systems to statistical attacks. In this method, the LSB of the pixels is mildly altered and used as a differentiator for pixels classification into groups (regular and singular). An increase in the embedding rate in a stego image should increase the differences between RM, R_M, and SM, S_M. The RS diagram [7] is used to detect the length of the embedding message. In Figure 5, (a) the difference between RM (SM) and R_M (S_M) increases with an increased embedding rate; hence, it can be detected. In (b), the difference between RM (SM) and R_M (S_M) remained the same with an increased embedding rate (showing small differences), and the length of the message cannot be detected [30].

6.2.2. Image histogram

The histogram is presented as a graph whose x-axis and y-axis explains the pixel difference between each pair and the number of occurrences, respectively. This attack is considered as one of the efficient experiments of a stego-image. Cover and stego-image histograms are usually compared to identify pixels distribution or to monitor unusual shapes as a result of an embedding algorithm. Figure 5 is a depiction of the histograms for 2 different schemes. The curves in each graph are depicted with solid lines while the histogram of the original images and those depicted with dotted lines represent the differences in the pixel histograms of the stego images. The step impact in the histogram clearly visualized the scheme earlier suggested in [36]. PVD-based steganographic approaches are mostly evaluated using different types of histogram analysis, including Histogram Characteristic Function - Center of Mass (HCF-COM) analysis and pixel difference histogram analysis [35-37].

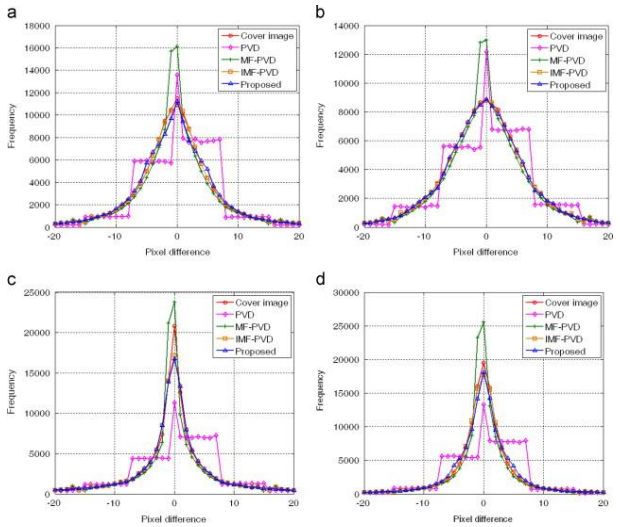


Fig. 6: Example Of Histogram Analysis For A- Lena, B- Peppers, C- House and D- Jet [36].

6.2.3. Confusion matrix

The major aim of steganalysis is mainly to determine whether a suspected medium is concealed with secret data. This implies that it mainly aims to ascertain the class of a testing medium (whether it belongs to the cover or stego class) [38]. There are four possible scenarios which could emerge if a specific steganalysis method is deployed for a suspicious medium analysis:

- A true positive (TP) scenario where a medium is rightly classified as a stego medium.
- A false negative (FN) scenario where a stego medium is wrongly classified as a cover.
- A true negative (TN) scenario where a cover medium is correctly classified as a cover.
- A false positive (FP) scenario where a cover medium is wrongly classified as a stego.

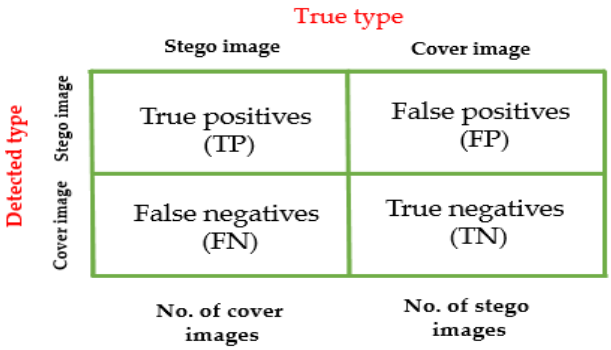


Fig. 7: Security Evaluation with Confusion Matrix.

6.2.4. Receiver operating characteristics (ROC)

The security of a steganalytic classifier can also be quantified with reference to ROC. With the ROC, the TP rate is plotted along the vertical (Y) axis while the FP rate is represented along the horizontal (X) axis (Figure 7). Given three steganalytic methods (Lower, TPF, and Upper), the Upper method is said to have a better steganalytic performance than the TPF method, while the TPF is better in performance than the Lower method. This is because the area under the ROC (AUC) curve is larger for Lower. Given the ROC curve:

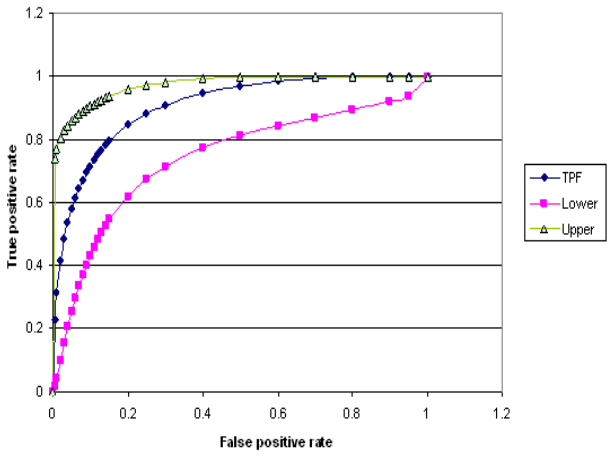


Fig. 8: Security Evaluation with ROC Curve.

6.3. Image quality measurement (IQM)

IQM are used to measure the image quality of the stego-images. The imperceptible of stego image must be high, means the distortion must be as low possible. The IQMs can be measured by utilizing different schemes as appeared in figure 4.

6.3.1. The mean-squared error (MSE)

The MSE between the original image (I1 (m,n)) and the stego-image (I2(m,n)) is computed by using (4) [39].

$$MSE = \frac{1}{M x N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2 \quad (1)$$

M and N are the number of rows and columns in the input images, respectively. The p_{ij} and q_{ij} are the carrier image pixel and the stego-image pixel value at i^{th} row and j^{th} column respectively. MSE of 100.0 for a grayscale image, looks awful, but an MSE of 100.0 for a 10-bit image (pixel values in [0,1023]) is hardly noticeable. The MSE should be as less possible. Whenever the MSE is equal to zero means both the carrier and the stego image are equal.

6.3.2. Root mean square error (RMSE)

The RMSE is usually applied as a measure of quality where can be computed utilizing (5).

$$\text{RMSE} = \sqrt{\frac{1}{M x N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2} \quad (2)$$

$$\text{RMSE} = \sqrt{MSE} \quad (3)$$

6.3.3. Signal-to-noise ratio (SNR)

The SNR is used to compare the desired signals' level to those of the background noise. The SNR refers to the ratio of signal power to the noise power and can be computed using equation 6.

$$SNR = 10x \log_{10} \left(\frac{\sum_{i=1}^{HxW} (Ci)^2}{\sum_{i=1}^{HxW} (Ci - Si)^2} \right) \quad (4)$$

6.3.4. Peak signal-to-noise ratio (PSNR)

This problem can be avoided by scaling the MSE based on the image range:

$$PSNR = 10x \log_{10} \left(\frac{Max^2}{MSE} \right) \quad (5)$$

Max = Maximum pixel intensity value which is 255.

The PSNR is measured and presented in decibels (dB). It is a good indicator for comparing the restoration results of the same image but meaningless across images. According to different studies, PSNR is ranked as follows: up to 40 dB = very good; 30 to 40 dB = acceptable; < 30 dB = not acceptable. The pixel of a color image comprises of 3 bytes and each byte is represented as a pixel [44,48].

6.3.5. The weighted peak signal-to-noise ratio (WPSNR)

The WPSNR is another quality measurement metric [45, 46] which uses a noise visibility function (NVF) parameter with MSE. The value of NVF must be in the range of zero (minimum) and one (maximum).

$$WPSNR = 10x \log_{10} \left(\frac{\left(Max\,(P\,(x,y)) \right)^2}{MSE\ x\ NVF} \right) \quad (6)$$

Where:

NVF= Noise Visibility

$$NVF = NORM \left(\frac{1}{1x (\wp_{Block})^2} \right) \quad (7)$$

$$\wp_{Block} = standard\ deviation\ of\ luminace\ of the\ pixel. \quad (8)$$

Where the local difference of the image is described by $\wp$ on the pixel who coordinate is (i , j).

6.3.6. The IQM using R measurement

The R measurement is used to calculate the resemblance between the carrier image and the stego image. It can be computed using equation 10 [44].

$$R = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - \bar{p}) x (q_{ij} - \bar{q})}{\sqrt{\left(\sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - \bar{p})^2 \right) x \left(\sum_{i=1}^{M} \sum_{j=1}^{N} (q_{ij} - \bar{q})^2 \right)}} \quad (9)$$

The $\bar{p}$ and $\bar{q}$ are respectively the carrier and stego images' medium pixel values. The function corr2 (p, q) determines the correlation between the carrier (p) and stego images (q). this function has a maximum value of 1 if p and q are the same image. Hence, lower distortions give higher correlations.

6.3.7. Image quality index (Q Index)

The stego-images are subjected to quality evaluation using the universal image quality index (Q Index) [40] which can be computed using (11). Mathematically, it is defined through a modeling of the image distortion with respect to the reference image based on 3 factors which are a loss of correlation, luminance distortion, and contrast distortion. The Q can have a maximum value of 1 only if p and q are the same images. They are defined in equations [12-14], and 15, respectively;

$$Q = \frac{4\,x\,(O'_{YZ})\,x\;Y''\,x\,Z''}{((O'_Y)^2+(O'_Z)^2)[(Y'')^2+(Z'')^2]} \tag{10}$$

$$Y'' = \frac{1}{N}\sum_{j=1}^{N} Y_j \;\;, Z'' = \frac{1}{N}\sum_{j=1}^{N} Z_j \tag{11}$$

$$(O'_Y)^2 = \frac{1}{N-1}\sum_{j=1}^{N}\left(Y_j - Y''\right)^2 \tag{12}$$

$$(O'_Z)^2 = \frac{1}{N-1}\sum_{j=1}^{N}\left(Z_j - Z''\right)^2 \tag{13}$$

$$O'_{YZ} = \frac{1}{N-1}\sum_{i=1}^{N}\left(Y_j - Y''\right)x\left(Z_j - Z''\right) \tag{14}$$

where ý represents the original images' mean pixel value, q represents the in stego-images' mean pixel value, $(O'_Y)^2$ and $(O'_Z)^2$ are the standard deviations for the carrier and stego images respectively, and O'_{YZ} is the covariance.

6.3.8. Structural information change (SSIM)

In this approach, the highly structured nature of the natural scene information is measured using the highly adaptable nature of HVS. The measure of the structural information change between the carrier and stego images (SSIM) [41] offers a good estimation of Perceived image distortion. Noted that when $C_1 = 0\; and\; C_2 = 0$, SSIM becomes equal to Q; thus, Q can be referred to as a special case of SSIM. All the B blocks of an images' SSIM is computed and the mean SSIM index determined to evaluate the overall image quality (17).

$$\mathrm{SSIM(x,y)} = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \tag{15}$$

$$\mu_x\,,\mu_y = mean\ intensities\ of\ cover\ and\ stego\ pixel\,.$$
$$\sigma_x\,,\sigma_y = mean\ intensities\ of\ cover\ and\ stego\ image\ block. \tag{16}$$

Note that when $C_1 = 0\; and\; C_2 = 0$,SSIM is equal to quality index Q. Thus, Q is a special case of SSIM. All the B blocks of the image SSIM is computed and then the mean SSIM index is calculated to evaluate the overall image quality, as in (17).

$$MSSIM = \frac{1}{B}\sum_{i=1}^{B} SSIM \tag{17}$$

6.3.9. Average difference (AD)

The simply refers to the average difference between the test image and the reference signal [42]. It is calculated using equation (18).

$$\mathrm{AD} = \frac{1}{HxW}\sum_{i=1}^{HxW}(C_i - S_i) \tag{18}$$

6.3.10. Image fidelity (IF)

The Image Fidelity (IF) is another metric for image quality measurement [47]. it can be Measurement by the equation (19).

$$\text{Image Fidelity (IF)} = 1 - \left(\frac{\sum_{i=1}^{HxW}(C_i\,x\,S_i)^2}{\sum_{i=1}^{HxW}(C_i)^2}\right) \tag{19}$$

6.3.11. Normalized cross correlation (NCC)

The NCC represents the proximity between two digital images; it can similarly be quantified in terms of correlation function [43]. The NCC can be measured using equation (20).

$$\mathrm{NCC} = \left(\frac{\sum_{i=1}^{HxW}(C_i\,x\,S_i)^2}{\sum_{i=1}^{HxW}(C_i)^2}\right) \tag{20}$$

7. Different evaluation of image formats

Many papers have been published in image steganography with different algorithms to select the best algorithm must analysis all factors within it. The different factors are selected in order to evaluate and analyze the file format for Steganography. The distortion of the image should not be visual to the human eye, where the payload capacity which is used to embed also plays a substantial role. Many testings within any algorithm is used in order to decide how much capacity of information could be used to embed. The steganalysis techniques are used to analyze the steganography methods and detecting the embedding information in the carrier image. The steganography methods should be more secure to stop against steganalysis algorithms. During sending the stego image, the intruder can check and manipulation the stego image to remove the embed information. This manipulation may can involve rotation, cropping and etc, of the carrier image. Must be chosen a steganographic algorithm to overcomes issue such manipulation and the steganographic information reaches the destination in the required format [48].

Many different methods have been proposed in this field, each method must be evaluating with different parameters to get an ideal method. Different steganography method has been published has been evaluated with different parameters, various methods are introduced within tables 2,3,4,5,6 and 7, in order to obtain a perfect method in image steganography.

Table 1: Comparison of Image Steganography Techniques

Cover Evaluation	LSB in BMP	LSB in GIF	LSB in PNG	JPEG	Spread Spectrum
Payload capacity	High	Moderate	Moderate	Moderate	Moderate
Security	Low	Low	Low	Moderate	High
IQAMs	High	Moderate	High	High	High
Image Manipulation	Low	Low	Low	Moderate	Moderate
unsuspicious file	Low	Low	Low	High	High

Table 2: Comparison of PSNR in Different Techniques

No. of Ref	Lena	Baboon	Peppers	House	Jet
FMM [50]	46.04	N/A	45.76	46.51	N/A
CST [51]	48.74	N/A	50.01	42.18	N/A
SHSI [52]	57.26	N/A	85.77	65.08	N/A
Ref [53]	49.95	N/A	50.05	54.36	N/A
MLSB-SM [54]	57	N/A	87.19	63.34	N/A
Ref [55]	54.43	N/A	56.11	N/A	N/A
DCT & OTP[56]	50.90	51.12	51.04	N/A	51.12
Ref [57]	49.08	49.12	N/A	N/A	56.11
Ref [58]	57.07	N/A	N/A	N/A	N/A
PVD & MF [59]	43.24	41.89	41.56	40.65	40.67
LSB& Data mapping [60]	48.41	48.34	48.31	46.34	47.53
Ref [61]	60.70	46.52	46.57	N/A	N/A

PIT [62]	47.19	N/A	17.44	42.23	N/A
Five modlus [63]	40.31	N/A	20.63	38.92	N/A
Ref [64]	47.05	N/A	17.44	42.18	N/A
GLM [65]	57.41	51.89	57.44	57.44	51.92
Ref [72]	49.97	N/A	50.06	50.06	N/A

Table 3: Comparison of Q Index in Different Techniques

Q index	Image	2K correction [73]	Ref [74]	Ref [67]	Cycling chaos [68]	Ref [69]	Ref [70]	3-dimensional CM [71]	PVD [75]	Ref [76]
	Baboon	0.9984	N/A	0.99935	0.99915	0.99905	0.99865	0.99967	N/A	N/A
	Lena	0.8323	0.7883	N/A	N/A	N/A	N/A	N/A	0.9227	0.7885
	Peppers	0.8569	0.8182	N/A	N/A	N/A	N/A	N/A	0.9449	0.8403
	F16 jet	0.9814	0.9813	N/A	N/A	N/A	N/A	N/A	0.9757	0.9495

Table 4: Comparison of Image Fidelity in Different Techniques

Image Fidelity	Image	Ref [57]	Edge detection [66]	Ref [67]	Cycling Chaos [68]	Ref [69]	Ref [70]	3-dimensional CM [71]
	Baboon	0.99	0.98756	0.99932	0.99912	0.99900	0.99100	0.99940

Table 5: Comparison of SSIM in Different Techniques

No of Ref.	Lena	Baboon	Peppers	House	Couple	Scene	Trees
FMM [50]	0.9822	0.9925	0.9488	0.986	0.9775	0.9817	0.9858
CST [51]	0.9993	0.995	0.989	0.9904	0.997	0.9909	0.998
SHSI [52]	0.9994	0.9998	0.9994	0.9904	0.9992	0.9996	0.9995
Ref [53]	0.9989	0.9992	0.8773	0.9989	0.998	0.9988	0.997
MLSB-SM [54]	0.9994	0.9998	0.9994	0.9995	0.9992	0.9996	0.9995
Ref [55]	0.7764	N/A	0.7764	N/A	N/A	N/A	N/A
Ref [58]	0.999919	N/A	N/A	N/A	N/A	N/A	N/A
PVD & MF [59]	0.844	0.816	0.799	0.810	N/A	N/A	N/A
LSB& Data mapping [60]	0.910	0.898	0.876	0.901	N/A	N/A	N/A
PIT [62]	0.9971	0.9985	N/A	0.9974	N/A	N/A	0.9956
Five modlus [63]	0.9822	0.9925	N/A	0.986	N/A	N/A	0.9858
Ref [64]	0.9989	0.9992	N/A	0.9989	N/A	N/A	0.997
GLM [65]	0.9994	0.9998	N/A	0.9995	N/A	N/A	0.9995

Table 6: Comparison of NCC in Different Techniques

No of Ref.	Lena	Baboon	Peppers	House	F16 jet	Trees	Moon
FMM 50	0.9994	0.999	N/A	0.9994	0.9993	0.9997	0.999
CST 51	0.9909	0.997	N/A	0.998	0.9993	0.874	0.989
SHSI 52	0.9996	0.9992	N/A	0.9995	0.9994	0.9998	0.9994
Ref [53]	1	0.9998	N/A	0.9999	0.9997	0.999	0.9998
MLSB-SM [54]	0.9993	0.9995	N/A	0.9996	0.9993	0.9994	0.9994
DCT & OTP [56]	1	1	1	N/A	1	N/A	1
Ref [58]	0.999493	N/A	N/A	N/A	N/A	N/A	N/A
Ref [72]	1	0.9998	N/A	0.9999	0.9997	0.999	0.9998

Table 7: Comparison of MSE in Different Techniques

No of Ref.	Lena	Baboon	Peppers	Scene	F16 jet
FMM 50	0.9964	N/A	N/A	1.0001	N/A
CST 51	0.0672	N/A	N/A	0.0783	N/A
SHSI 52	0.0738	N/A	N/A	0.0737	N/A
Ref [53]	0.0768	N/A	N/A	0.0767	N/A
MLSB-SM [54]	0.0008	N/A	N/A	0.0001	N/A
DCT & OTP [56]	0.5273	0.5020	0.5107	N/A	0.5020
Ref 57	1.01	1.00	N/A	0.08	0.15
PVD & MF [59]	3.08	4.21	4.45	N/A	5.572
LSB& Data mapping [60]	0.938	0.952	0.956	N/A	1.148
Ref [61]	0.055	1.447	1.433	N/A	N/A
Ref [77]	0.48	0.26	N/A	N/A	N/A
LSB [78]	0.0743	0.0741	0.0747	N/A	N/A
MLTS [79]	0.0211	0.0214	0.0212	N/A	N/A
Ref [80]	17.01	15.89	N/A	N/A	15.47
LSB Modification [81]	2.28	2.28	N/A	N/A	2.34

8. Some directions in future

The substantial directions for future realizations include:

i) An appropriate combination of the LSB, PVD, and EMD approaches.
ii) A multi-directional edge with a random selection.
iii) An YCbCr color model should be used.
iv) Minimizing the additive noise distortion function.

The LSB replacement can be extended up to 4 LSB bits to obtain a higher hiding capacity. The PVD schemes offer a smooth block and embed the intended number of bits; thus, it offers more security. The LSB and PVD schemes are combined to achieve a maximum embedding capacity and a better security [82, 83]. The implementation of the combined LSB-PVD scheme as suggested by [84] provides a higher embedding capacity and a better PSNR. Recent studies have reported a better achievement using a combined PVD and EMD schemes [85]. Therefore, the LSB, PVD, and EMD schemes can be work together to achieve a higher embedding capacity, higher security, and a lower distortion rate. The LSB of steganography within RGB color image can differently performed by considering each of the RGB components individually and replacing their LSB planes. The RGB color image can be

utilized as a carrier with LSB and PVD in a different manner through handling each of the RGB components separately. Moreover, the security and payload capacity can be realized by using the vertical, horizontal, and diagonal edges. Watermarking refers to the act of embedding a carrier file with information to ensure ownership protection. The YCbCr model is commonly used in watermarking [86] and can also be used in steganography to resist current steganalysis attacks. In general, modern steganalysis aims at computing the specific features of stego and cover images to differentiate their classes. Most of these specific features are generated through the incorporation of noise in stego images. There is still a need for more efforts towards exploring and minimizing the introduction of noise while designing new steganographic techniques [87], [88].

9. Conclusion

This paper is a narration of all the measurement metrics that used mathematical equations in image steganography. To propose a new steganography scheme, there is a need to evaluate its performance based on 3 parameters which are the hiding capacity, the security, and the distortion measure. This work also presented different steganalysis tools, such as RS and pixel difference histogram analyses for security evaluation. Some directions for future investigations were also provided in this work.

Acknowledgement

THIS PAPER IS A PORTION OF A VAST RESEARCH SUPPORTED BY FACILITY OF COMPUTING, UNIVERSITY TECHNOLOGY MALAYSIA. THE AUTHORS WOULD LIKE TO EXPRESS MY DEEPEST APPRECIATION TO ALL REVIEWERS FOR THEIR INSIGHTFUL COMMENTS AND SUGGESTIONS FOR A BETTER RESEARCH.

References

[1] HASHIM, M., RAHIM, M., SHAFRY, M., & ALWAN, A. A. (2018). A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. Journal of Theoretical & Applied Information Technology, 96(4).

[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[3] MAHDI HASHIM, M. O. H. A. M. M. E. D., RAHIM, M., & SHAFRY, M. (2017). IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION. Journal of Theoretical & Applied Information Technology, 95(22).

[4] Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. IEEE multimedia, 8(4), 22-28. https://doi.org/10.1109/93.959097.

[5] Swain, G., & Lenka, S. K. (2015). A novel steganography technique by mapping words with LSB array. International Journal of Signal and Imaging Systems Engineering, 8(1-2), 115-122. https://doi.org/10.1504/IJSISE.2015.067052.

[6] Swain, G., & Lenka, S. K. (2012). LSB array based image steganography technique by exploring the four least significant bits. In Global Trends in Information Systems and Software Applications (pp. 479-488). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29216-3_52.

[7] Swain, G., & Lenka, S. K. (2012). A technique for secret communication using a new block cipher with dynamic steganography. International Journal of Security and Its Applications, 6(2), 1-12.

[8] Swain, G., & Lenka, S. K. (2012). A robust image steganography technique using dynamic embedding with two least significant bits. In Advanced Materials Research (Vol. 403, pp. 835-841). Trans Tech Publications.

[9] Subhedar, M. S., & Mankar, V. H. (2014). Status and key issues in image steganography: A survey. Computr science review, 13, 95-113. https://doi.org/10.1016/j.cosrev.2014.09.001.

[10] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66. https://doi.org/10.1016/j.image.2018.03.012.

[11] ECE, C., & Mullana, M. M. U. (2011). Image quality assessment techniques pn spatial domain. IJCST, 2(3).

[12] Simmons, G. J. (1984). The prisoners' problem and the subliminal channel. In Advances in Cryptology (pp. 51-67). Springer, Boston, MA. https://doi.org/10.1007/978-1-4684-4730-9_5.

[13] Knuth, D. E. (1985). Dynamic huffman coding. Journal of algorithms, 6(2), 163-180. https://doi.org/10.1016/0196-6774(85)90036-7.

[14] T. Sharp, \Hide 2.1, 2001," http://www.sharpthoughts.org

[15] G. Pulcini, \Stegotif," http:// www.geocities.com/ SiliconValley /9210 /gfree.html

[16] Ulker, M., & Arslan, B. (2018, March). A novel secure model: Image steganography with logistic map and secret key. In Digital Forensic and Security (ISDFS), 2018 6th International Symposium on (pp. 1-5). IEEE.

[17] Sarmah, D. K., & Kulkarni, A. J. (2018). JPEG based steganography methods using Cohort Intelligence with Cognitive Computing and modified Multi Random Start Local Search optimization algorithms. Information Sciences, 430, 378-396. https://doi.org/10.1016/j.ins.2017.11.027.

[18] Li, B., Li, Z., Zhou, S., Tan, S., & Zhang, X. (2018). New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator. IEEE Transactions on Information Forensics and Security, 13(5), 1242-1257. https://doi.org/10.1109/TIFS.2017.2780805.

[19] Zhang, Y., Qin, C., Zhang, W., Liu, F., & Luo, X. (2018). On the fault-tolerant performance for a class of robust image steganography. Signal Processing, 146, 99-111. https://doi.org/10.1016/j.sigpro.2018.01.011.

[20] Panghal, S., Kumar, S., & Kumar, N. (2016). Enhanced Security of Data using Image Steganography and AES Encryption Technique. International Journal of Computer Applications (0975–8887) Recent Trends in Future Prospective in Engineering & Management Technology 2016.

[21] Debnath, B., Das, J. C., & De, D. (2017). Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication. IET Circuits, Devices & Systems, 11(1), 58-67. https://doi.org/10.1049/iet-cds.2015.0245.

[22] AbdelQader, A., & AlTamimi, F. (2017). ANovel IMAGE STEGANOGRAPHY APPROACH USING MULTI-LAYERS DCT FEATURES BASED ON SUPPORT VECTOR MACHINE CLASSIFIER. The International Journal of Multimedia & Its Applications. https://doi.org/10.5121/ijma.2017.9101.

[23] Kennedy, J. H., Khan, M. T. A., Ahmed, M. J., & Rasool, M. D. (2017). Image Steganography Based on AES Algorithm with Huffman Coding for Compressionon Grey Images. International Journal of Engineering Science and Computing, [7].

[24] Das, R., & Chatterjee, P. (2017, March). Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography. In Proceedings of the International Conference on High Performance Compilation, Computing and Communications (pp. 17-22). ACM.

[25] Tiwari, N., & Shandilya, D. M. (2010). Evaluation of various LSB based methods of image steganography on GIF file format. International Journal of Computer Applications (0975–8887) Volume. https://doi.org/10.5120/1057-1378.

[26] Reddy, H. M., & Raja, K. B. (2011). Wavelet based non-LSB steganography. International Journal of Advanced networking and applications, 3(3), 1203.

[27] HASHIM, M., RAHIM, M., SHAFRY, M., & ALWAN, A. A. (2018). A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. Journal of Theoretical & Applied Information Technology, 96(4).

[28] Swain, G. (2018). Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. Arabian Journal for Science and Engineering, 1-10.

[29] Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. (2017). CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications, 76(6), 8597-8626. https://doi.org/10.1007/s11042-016-3383-5.

[30] Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. IEEE multimedia, 8(4), 22-28. https://doi.org/10.1109/93.959097.

[31] Joyce, J. M. (2011). Kullback-leibler divergence. In International encyclopedia of statistical science (pp. 720-722). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04898-2_327.

[32] Cachin, C. (1998, April). An information-theoretic model for steganography. In International Workshop on Information Hiding (pp. 306-318). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-49380-8_21.

[33] Borgwardt, K. M., Gretton, A., Rasch, M. J., Kriegel, H. P., Schölkopf, B., & Smola, A. J. (2006). Integrating structured biological data by kernel maximum mean discrepancy. Bioinformatics, 22(14), e49-e57. https://doi.org/10.1093/bioinformatics/btl242.

[34] Holub, V., & Fridrich, J. (2013, June). Digital image steganography using universal distortion. In Proceedings of the first ACM workshop on Information hiding and multimedia security (pp. 59-68). ACM. https://doi.org/10.1145/2482513.2482514 .

[35] Wang, Y., Chen, Q., & Zhang, B. (1999). Image enhancement based on equal area dualistic sub-image histogram equalization method. IEEE Transactions on Consumer Electronics, 45(1), 68-75. https://doi.org/10.1109/30.754419.

[36] Chen, J. (2014). A PVD-based data hiding method with histogram preserving using pixel pair matching. Signal Processing: Image Communication, 29(3), 375-384. https://doi.org/10.1016/j.image.2014.01.003.

[37] Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. IEEE signal processing letters, 12(6), 441-444. https://doi.org/10.1109/LSP.2005.847889.

[38] Nguyen, B. C., Yoon, S. M., & Lee, H. K. (2006, November). Multi bit plane image steganography. In International Workshop on Digital Watermarking (pp. 61-70). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11922841_6.

[39] Swain, G., & Lenka, S. K. (2014). Classification of image steganography techniques in spatial domain: a study. International Journal of Computer Science & Engineering Technology, 5(3), 219-232.

[40] Wang, Z., & Bovik, A. C. (2002). A universal image quality index. IEEE signal processing letters, 9(3), 81-84. https://doi.org/10.1109/97.995823.

[41] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing, 13(4), 600-612. https://doi.org/10.1109/TIP.2003.819861.

[42] Kumar, R., & Rattan, M. (2012). Analysis of various quality metrics for medical image processing. International Journal of Advanced Research in Computer Science and Software Engineering, 2(11).

[43] Avcibas, I., Memon, N., & Sankur, B. (2003). Steganalysis using image quality metrics. IEEE transactions on Image Processing, 12(2), 221-229. https://doi.org/10.1109/TIP.2002.807363.

[44] Swain, G., & Lenka, S. K. (2014). Classification of spatial domain image steganography techniques: a study. International Journal of Computer Science & Engineering Technology, 5(3), 219-232.

[45] Al-Dmour, H., & Al-Ani, A. (2016). A steganography embedding method based on edge identification and XOR coding. Expert systems with Applications, 46, 293-306. https://doi.org/10.1016/j.eswa.2015.10.024.

[46] Sau, K., Basak, R. K., & Chanda, A. (2013). Image compression based on block truncation coding using clifford algebra. Procedia Technology, 10, 699-706. https://doi.org/10.1016/j.protcy.2013.12.412.

[47] Krenn, R. (2004). Steganography and steganalysis.

[48] Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications*, *77*(13), 17333-17373. https://doi.org/10.1007/s11042-017-5308-3.

[49] MAHMOOD, A. S., RAHIM, M., & SHAFRY, M. (2017). GENERATING AND EXPANDING OF AN ENCRYPTION KEY BASED ON KNIGHT TOUR PROBLEM. *Journal of Theoretical & Applied Information Technology*, *95*(7).

[50] Jassim F A (2013) A novel steganography algorithm for hiding text in image using five modulus methods. arXiv preprint arXiv:1307.0642.

[51] Muhammad K, Ahmad J, Rehman NU, Jan Z, Qereshi RJ (2014) A secure cyclic steganographic technique for color images using randomization. Tech J Univ Eng Technol Taxila Pakistan 19:57–64.

[52] Muhammad K, Ahmad J, Farman H, Zubair M (2014) A novel image steganographic approach for hiding text in color images using HSI color model. Middle-East J Sci Res 22:647–654.

[53] Karim M (2011) a new approach for LSB based image steganography using secret key. In: 14th International Conference on Computer and Information Technology (ICCIT 2011). pp 286–291 https://doi.org/10.1109/ICCITechn.2011.6164800.

[54] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimedia Tools and Applications, 75(22), 14867-14893. https://doi.org/10.1007/s11042-015-2671-9.

[55] Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. Procedia Computer Science, 46, 612-618. https://doi.org/10.1016/j.procs.2015.02.105.

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

[57] Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., & Dutta, P. (2014). A novel secure image steganography method based on Chaos theory in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1), 11-22. https://doi.org/10.5121/ijsptm.2014.3102.

[58] Çataltaş, Ö. & Tütüncü, K. (2017, September). Comparison of LSB image steganography technique in different color spaces. In Artificial Intelligence and Data Processing Symposium (IDAP), 2017 International (pp. 1-6). IEEE.

[59] Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software, 81(1), 150-158. https://doi.org/10.1016/j.jss.2007.01.049.

[60] Dhar, P. K., Kaium, A., & Shimamura, T. (2018). Image Steganography Based on Modified LSB Substitution Method and Data Mapping. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18(3), 155-160.

[61] Juneja, M., & Sandhu, P. S. (2013). A new approach for information security using an improved steganography technique. Journal of Information Processing Systems, 9(3), 405-424. https://doi.org/10.3745/JIPS.2013.9.3.405.

[62] Adnan Abdul-Aziz Gutub, "Pixel Indicator Technique for RGB Image Steganography," Journal of Emerging Technologies in Web Intelligence, Vol. 2, No. 1, pp. 56-64, February 2010. doi:10.4304/jetwi.2.1.56-64 https://doi.org/10.4304/jetwi.2.1.56-64.

[63] Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five-modulus method. arXiv preprint arXiv:1307.0642.

[64] Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In Computer and Information Technology (ICCIT), 2011 14th International Conference on (pp. 286-291). IEEE.

[65] Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W. (2015). A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS, 9(5), 1938-1962.

[66] Alam, S., Kumar, V., Siddiqui, W. A., & Ahmad, M. (2014, February). Key dependent image steganography using edge detection. In Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on (pp. 85-88). IEEE.

[67] Anees, A., Siddiqui, A. M., Ahmed, J., & Hussain, I. (2014). A technique for digital steganography using chaotic maps. Nonlinear Dynamics, 75(4), 807-816. https://doi.org/10.1007/s11071-013-1105-3.

[68] Aziz, M., Tayarani-N, M. H., & Afsar, M. (2015). A cycling chaos-based cryptic-free algorithm for image steganography. Nonlinear Dynamics, 80(3), 1271-1290. https://doi.org/10.1007/s11071-015-1943-2.

[69] Ghebleh, M., & Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898-1907. https://doi.org/10.1016/j.cnsns.2013.10.014.

[70] Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., & Dutta, P. (2014). A novel secure image steganography method based on Chaos theory in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1), 11-22. https://doi.org/10.5121/ijsptm.2014.3102.

[71] Sharif, A., Mollaeefar, M., & Nazari, M. (2017). A novel method for digital image steganography based on a new three-dimensional chaotic map. Multimedia Tools and Applications, 76(6), 7849-7867. https://doi.org/10.1007/s11042-016-3398-y.

[72] Bailey, K., & Curran, K. (2006). An evaluation of image based steganography methods. Multimedia Tools and Applications, 30(1), 55-88. https://doi.org/10.1007/s11042-006-0008-4.

[73] Yu, J. G., Yoon, E. J., Shin, S. H., & Yoo, K. Y. (2008, April). A new image steganography based on twok correction and edge-detection. In Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on (pp. 563-568). IEEE.
[74] Lie, W. N., & Chang, L. C. (1999). Data hiding in images with adaptive numbers of least significant bits based on the human visual system. In Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on (Vol. 1, pp. 286-290). IEEE.
[75] Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10), 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6.
[76] Chandramouli, R., Kharrazi, M., & Memon, N. (2003, October). Image steganography and steganalysis: Concepts and practice. In International Workshop on Digital Watermarking (pp. 35-49). Springer, Berlin, Heidelberg.
[77] Dhaka, V., Poonia, R. C., & Singh, Y. V. (2013). A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8).
[78] Singh, A., & Singh, H. (2015, March). An improved LSB based image steganography technique for RGB images. In Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on (pp. 1-4). IEEE.
[79] Chauhan, S., Kumar, J., & Doegar, A. (2017, February). Multiple layer text security using variable block size cryptography and image steganography. In Computational Intelligence & Communication Technology (CICT), 2017 3rd International Conference on (pp. 1-7). IEEE.
[80] Khodaei, M., & Faez, K. (2010, June). Image hiding by using genetic algorithm and LSB substitution. In International Conference on Image and Signal Processing (pp. 404-411). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13681-8_47.
[81] Rajendran, S., & Doraipandian, M. (2017). Chaotic Map Based Random Image Steganography Using LSB Technique. IJ Network Security, 19(4), 593-598.
[82] Wu, H. C., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings-Vision, Image and Signal Processing, 152(5), 611-615. https://doi.org/10.1049/ip-vis:20059022.
[83] Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2010). Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. Journal of Systems and Software, 83(10), 1635-1643. https://doi.org/10.1016/j.jss.2010.03.081.
[84] Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image processing, 6(6), 677-686. https://doi.org/10.1049/iet-ipr.2011.0059.
[85] Shen, S. Y., & Huang, L. H. (2015). A data hiding scheme using pixel value differencing and improving exploiting modification directions. Computers & Security, 48, 131-141. https://doi.org/10.1016/j.cose.2014.07.008.
[86] Lusson, F., Bailey, K., Leeney, M., & Curran, K. (2013). A novel approach to digital watermarking, exploiting colour spaces. Signal Processing, 93(5), 1268-1294. https://doi.org/10.1016/j.sigpro.2012.10.018.
[87] Balasubramanian, C., Selvakumar, S., & Geetha, S. (2014). High payload image steganography with reduced distortion using octonary pixel pairing scheme. Multimedia tools and applications, 73(3), 2223-2245. https://doi.org/10.1007/s11042-013-1640-4.
[88] Li, B., Wang, M., Huang, J., & Li, X. (2014, October). A new cost function for spatial image steganography. In Image Processing (ICIP), 2014 IEEE International Conference on (pp. 4206-4210). IEEE.