Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFECTIVE AND SECURE DIGITAL IMAGE STEGANOGRAPHY SCHEME USING TWO RANDOM FUNCTION AND CHAOTIC MAP

[1]MOHANAD NAJM ABDULWAHED

[1]Materials department, University of Technology, Baghdad, Iraq

E-mail: mohanadnajmabdulwahed@gmail.com

ABSTRACT

Among the critical features of actions and strategies in the information and communications technology period is securing information. The reliability of information ought to be the main consideration in the discrete transfer of information between two people. For the security of information, the approaches entail steganography and cryptography. In cryptography, the discrete information is changed into indiscernible information yet still the secret information is recognizable, while steganography is about concealing the secret text to avoid it being discerned. This paper presents a current secure image steganography method called new stego key adaptive LSB (NSKA-LSB). The establishment of the suggested method was built in four stages with an objective of a better data-hiding algorithm in cover image identity using potentiality, image aspects, and reliability. Attaining this involves preserving the Peak Signal-to-Noise Ratio (PSNR) of the steganography method. The four-stage proceeded with pixel determination assembly stage, then secret information assembly stage, embedding stage and lastly extrication stage. The reliable image steganography method suggested in this paper is established on a novel transformation of least significant bit exchange technique, a fusion of two arbitrary functions, and a chaotic map. The suggested method entails direct or inverse discrete bit positioning of strengthening the invisibility and difficulty of the insertion exercise. The reason for suggesting the hiding algorithm is to tackle statistical and visual types of attacks. The investigations outcomes exhibit that the formula gives the improved quality index, peak signal-to-noise ratio, and payload employed for stego image examination.

Keywords: *Image steganography Bernoulli's map, PSNR, SSIM, RLE*

1. INTRODUCTION

There is an uprising security dispute in sending sensitive messages over a universal web, plus becoming a captivating study topic previously. As a result, engaging cryptography, which is about encoding delicate messages into unfamiliar information is incorporated to solve this difficulty of message reliability [1]. Nonetheless, there is the issue of meaningless for the encrypted information that draws the mindfulness of unauthorized persons because of the disreputable nature of the information. Any reckon by the strikers on the availability of a message, effectual cryptanalysis structures are employed for decrypting the information [8]. Employing techniques for concealing such messages ought to provide solution, and this entails steganography with the potentiality to shield messages during conveyance, with less reliability infringement [14,2].

Steganography, an art of science for discrete conveyance, is a peculiar method of shielding messages. Its objective is concealing secret information within a cover image to avoid visibility to an attacker with visibility to only the transmitter and beneficiary of the information who have message reality realization [3,13]. The central principles of steganography entail a text, a carrier object, hiding technique and a stego key for improved security [6,7]. The carrier object entails embedding information which ought to be text, audio or video. Employing steganography can happen in a wide span of approaches inclusive of reliable conveyance of secret military information and other intelligence organizations, strengthening mobile banking reliability, reliability of online voting, and conceal disclosure between two relaying parties [5].

Steganography can be effectively used in different applications, but using it can be quite risky because attackers can use it to send Trojans and viruses with the aim of compromising sensitive systems. More so, with the use of this information-

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

hiding technology, criminals or terrorists may be enabled to exchange secrete information [7].

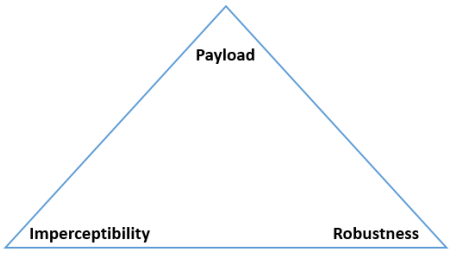

Figure 1. The steganography triangle requirement model

As illustrated in figure1, payload is described as the amount of secrete data which can be concealed within a cover object successfully without creating visual artifacts in stego images. The size of the payload is directly proportional to the strength of steganography algorithm and vice versa [1]. In steganography, the word robustness refers to the resilience of a steganography algorithm against diverse kinds of statistical and simple attacks. if the data that is hidden in a cover image cannot be easily modified or extracted using image processing operations, then the steganography algorithm used is regarded as robust. Some of the image processing operations that can be used in the modification or extraction of concealed messages include scaling, cropping, image rotation, and noising [9]. The concept of imperceptibility is synonymous to undectability, which can be measured using diverse metrics of image quality assessment like structural-index metric (SSIM) and peak-signal-to-noise-ratio (PSNR). The imperceptibility of a method of steganography is high if it is able to produce images that can barely be distorted after data has been intentionally concealed in a manner that it cannot be easily detected by the use of human visual system (HVS) [15, 11].

In the last ten year, so many spatial domain steganography methods have been proposed by researchers, and one of the widely known ones is Least Significant Bit (LSB) replacement. With this scheme, a replacement of the host mage with message is done, and thus, yielding a comparatively good quality marked image. Nevertheless, it allows comparatively easy detection using steganalysis methods because of its simplicity and the imbalanced pixel modification [17]. In order to reduce this limitation, the use of LSB-matching (LSBM) scheme [16] is employed in making an addition or a subtraction of a numerical one to the pixels of the host image based on the secrete message. This in turn minimizes the probability of message detection, but with distortion of marked images. The LSBM scheme was modified and named LSBM revisited (LSBMR) [18], in which the correlation between a pair of pixels is considered as a means of hiding two bits at the same time, thereby minimizing the rate of distortion for marked images to 0.325 from 0.5 bpp or 6.25% EP. In order to further reduce the detectability of marked images, Luo et al. [16], combined the LSBMR with edge-based data hiding mechanism. In their part, the areas of cover image were selected adaptively for hiding message based on the requirements. Regardless of the benefits offered by these methods, they are vulnerable the problems like: a) directly using the host image to embed sensitive information without encryption, thereby enhancing the operation of attackers in terms of extracting the secret messages more easily by cracking the embedding algorithm, b) the use of ineffective embedding algorithms can produce visually distorted stego images, which in turn increases the probability of detection by human visual system, and c) imbalance between quality of image, computational complexity, payload and security, thereby making them inappropriate for use in real-time and top-secret security applications.

The criteria that have been adopted in this paper are discussed according to the key contributions:

1. Propose a secure steganography scheme which combines the benefits of chaotic method and compression with the aim of achieving a better balance between the quality of image, payload and security, thus, enhancing the suitability of the proposed scheme for use in real-time and top-secret level security applications.

2. The use of Fibonacci technique is employed in converting the bitplane of cover image from 8-bitplane to 12-bitplanes because of binary representation. This is more appropriate for the process of embedding in terms of stego-image imperceptibility, while the robustness of data embedding is enhanced.

3. Using Bernoulli's map before the process of data embedding to chaotic sensitive information. The aim of this is to introduce an additional obstacle for attackers, therefore, maintaining high level of security for secret information regardless of if the core steganography algorithm is cracked.

4. The Run-Length Encoding (RLE) compression has been used to enhance the compression process and reduced the secret message before embedding process.

5. Identifying the random pixel that can be used in embedding secret information, while the two random

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

functions are utilized in enhancing the resilience of the system against the attempts of trackers to uncover which pixel to embed first or the sequence of pixels.

6. Proposed a new scheme called new stego key adaptive LSB (NSKA-LSB) to embed secret message within cover image. In this scheme, the visual quality of the stego images is enhanced while the extraction of data is made difficult, thereby reducing the detectability by HVS.

This paper is made up of different sections as follows: Section 2 presents related work discussions on the conventional LSB steganography, random map function, chaotic method and Fibonacci decomposition. In Section 3, the proposed scheme is described in detail. Section 4 presents the results of experiments and analysis conducted in this paper. Lastly, Section 5 presents the conclusion of the paper.

2. RELATED WORK

This section consists different sub-section that related to our work based different techniques.

.

2.1. least significant bit substitution (LSB)

Least significant bit (LSB) substitution is a conventional and simple method used to insert secret information within a cover image [19]. While this process is ongoing, it is possible to overwrite the binary representation of the secret data. With regards to the gray-scale images whose pixels possess just a single value ranging from 0 to 255 and the bit depth of 8 bits, the bits of the secret information cannot be converted into binary bits because they are used directly to substitute the cover object's image. Pertaining the colour images that possess 3 routes (RGB) and the bit depth of 24 bits, the cover object (image) is initially divided into 3 channels before the secret information is embedded in each of the channels. Finally, the three paths are merged so as to produce the stego image. The modification of the LSB bits does not allow the HVS to detect the stego-image. Due to the fact that a distinct kind of the LSB substitution method is utilized in the proposed scheme, a mathematical expression of the method is provided with adequate details. The aim of this mathematical expression is to provide deeper insight on the central idea of the scheme in section 3. Diverse embedding percentage (EP) of LSB, which include 6.25% and 12.5%, which means 0.5 and 1.0 bpp respectively are used based on the capacity that is to be embedded.

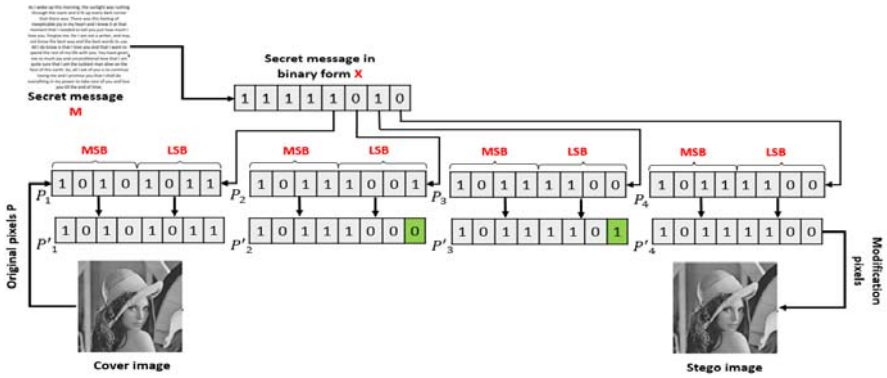

Figure 2. Simple LSB substitution procedure.

Through the use of a simple instance, a comprehensive explanation of the central idea of the LSB-based steganography is provided: it is assumed that P is a grayscale image consisting of 8 pixels [P=P_1, P_2, P_3, P_4] with the next values for their decimal and an associated binary substitutions as given in figure 2.
Where M denotes the secret text, in a manner that M= 'A' with the binary form X= 01000001. For X to be embedded within a certain cover image P, a replacement of the pixels' LSB [P =P_1, P_2, P_3, P_4] is made with the bits of M (01000001), and the pixel which is obtained after the secret message has been embedded is denoted by [P =P'_1, P'_2, P'_3,P'_4] with their decimal and associated binary values as given in figure 2. The LSB in the pixels [P =P'_1, P'_2, P'_3, P'_4] are the pixels that have been modified and are the products of the process of embedding. This an example of 12.5% EP which means 1bpp in each LSB, which can be expanded to different EP. This way, the imperceptibility of the stego image is reduced, thereby making it easy

© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for the HVS to detect the stego-image. Here, image quality is compromised for data capacity. If a larger amount of data is concealed, degradation occurs in the image quality. With the use of LSB methods, high data capacity is achieved.

$$P_c = \begin{cases} P_s - 1 & ,if\ A \neq LSB\ (P_s)\ \text{and}\ P_s\ \text{is Even} \\ P_s + 1 & ,if\ A \neq LSB\ (P_s)\ \text{and}\ P_s\ \text{is Odd} \\ P_s & ,if\ A = LSB\ (P_s) \end{cases} \quad (1)$$

Where, P_c and P_s represent the stego and cover image pixel values respectively, and A is the desired bit value of the secret message [20].

In reference [4], a secure image steganography based on Huffman coding, odd/even distribution, and henon map. In comparison to other extant methods, the implementation of the proposed system was found to be less complex. In order to improve the system's security, the use of the henon map algorithm was employed, the imperceptibility of the stego-image is enhanced by using odd/even distribution. Prior to the process of embedding, the secrete message is embedded using Huffman coding. There are two major reasons why this method is considered effective: the first is it is capable of checking the correspondence between secret bits with LSB and mapping so as to ascertain odd and even word during the process of embedding, and the second one is the segmentation of the secret message with the aim of tracking and mapping every bit within the stego image. Based on the results, the performance of their proposed method is better than that of [21] in terms of PSNR.

In reference [21], an edge-based method of embedding secret image was proposed by the authors, and the method was used together with the canny edge detector alongside 2k correction (the visual quality was maintained by 2k correction). With this technique, the edge of the cover image was detected using the canny edge detector, and the secret data was embedded in just the edge pixels. Secondly, the authors enhanced the security by randomizing the edge pixels through the use of a sorting technique. The computation of an adaptive coherent bit length L was performed and determined using the edge pixels which are also used in replacing secret data. Despite the fact that works previously done in this area have achieved high capacity and visual quality of stego-images, detecting using state-of-the-art steganalysis could be easy. More so, thorough computation is required because of the encoding phase with regards to other extant spatial domain method.

In reference [22], a technique for colour images with the aim of enhancing the visual imperceptibility and embedding payload has proposed. The technique is a three-phase intelligent technique involving one phase before the process of embedding and the other two phases after the process of embedding. The first phase involves the application of a learning system (LS) prior to the process of embedding, and the other two phases involve the use of adaptive GA and ANN when the process of embedding is completed. The aim of using the ANN and the adaptive GA is to enable the estimation of the secrete bits within the pixels. Based on the results, the proposed algorithm demonstrated the capability of embedding a larger payload of up to 12 bpp with high visual quality.

In other reference that carried out by Liao et al. [23], two new RTB methods known as CRT (cubic reference table) and CRT-PVD (cubic reference table and pixel value differencing) were proposed. These methods can be considered as a broad coverage of the previous works for x-dimensional reference table framework. While the cubic reference table (CRT) is independent of image contents, the cubic reference table and pixel value differencing (CRT-PVD) is dependent on the distinguished image sleekness. Since the dimensional space is a limitation for the pixels that need to be embedded, the authors in their proposed method expanded the dimensional space of the reference table. The performance of the proposed method is evaluated by means of theoretical analyses.

In reference [25], a bit-flipping method was proposed by the authors to enable the hiding of secret data within the original image. In this method, a block is made up of 2 pixels with one of two LSBs being flipped for the purpose of concealing secret information in it. There are two variants, of which Variant-1 and Variant 2 utilize 7th and 8th bit of a pixel to hide secret data. With Variant-1, 3-bits are hidden in a pair of pixels, while in Variant-2 4-bits are hidden in a pair of pixels. Our proposed method notably raises the capacity as well as bits per pixel that can be hidden in the image compared to existing bit flipping method.

In the study [24], Muhammad et al. instigated the steganography strategy that brings image invisibility. The strategy is termed as a pattern-based shuffling algorithm (PBSA) and is incorporated for grayscale images in spatial discipline. Employing this algorithm entails

© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

incorporation of a secret key for encrypting and secret data mixing with the encoded information being embedded within the cover image by employing M-LSB technique. Further study show, suggestion of a bit-flipping technique by the researchers for discrete information concealing within the original image [10]. This technique is about twisting a block of 2 pixels with one of two LSBs for discrete data concealing. There are two variants, of which Variant-1 and Variant 2 employ 7th and 8th bit of a pixel to conceal discrete information. The suggested method primarily increases the volume as well as bits per pixel able to be concealed in the image in contrast to prevailing bit flipping technique.

2.2. Random function.

Many studies have been carried out in steganography with the aim of developing, novel methods through which messages can be secured using steganography [4]. For the purpose of enhancing data privacy, many such studies have used the random technique because of its higher efficiency and ease of use. The following are the advantages of randomized algorithm:

- Rapid and ease, or even both for diverse problems.
- Easy implementation.
- Rapid with high probability, and/or
- Produces optimum output with very high probability.

In the literature, it has been found that several authors have leveraged the advantages of the random maps function, with each having its shortcomings and strengths. Based on behavior, there are diverse kinds of random maps in existence, and they include, NUBASI [26], Arnold scrambling [27], LDA [28], Henon map [29] and Knight Tour [21]. In normal random maps, the number is selected using single parameter, with the initial condition of this function being (single) is 10^{15}, while the possibility of discovering these numbers is 2^{50} [29]. three random maps are used for the allocation of pixels with the aim of maintaining the proposed work.

2.3 Chaotic Maps Function

One of the emerging areas in steganography is combining steganography with chaotic method, and the attention of researchers is being attracted to this development. In recent times, the role played by chaotic systems in several applications in the field of nonlinear systems has become essential [30, 31]. A description of the set of chaotic system properties is given in the chaos methods [32-34]. Some of these vital properties are outlined in table 1.

Table 1. Different properties of chaotic methods.

	Chaotic system properties	Comment
1.	Ergodicity and Missing Property	There seems to be similarity between the outputs of chaotic system any type of input.
2.	Sensitivity to Initial Condition	When there is a small variation in the input, it results in the production of larger variation in the output.
3.	Deterministic and Complexity	Produces a complex output in form of pseudo-randomness.

The benefits of random techniques have been leveraged by numerous authors in the literature, and the review of literature showed that some of these random techniques possess very efficient algorithms, while the remaining have fewer number generating facilities. The use of such techniques of number-generating key has also been employed in different tasks for chaotic maps in several areas, particularly in security and for processing images. There are different kinds of chaotic maps which include Bernoulli map, tent map and logistic map, these maps all exist based on the behaviour [35]. In proposed scheme, Bernoulli's map is used for generating chaotic cipher message of the secret message. In a chaotic system, secret message is encrypted using chaotic sequence, which serves as a key. The use of chaotic map is used in generating the key, while the use of the initial key is employed in creating a chaotic sequence . Such kinds of systems are more appropriate for use with large amounts of data. Key generation was technique was used in study [33] to change the message to cipher text through the use of the message and key.

2.4 Fibonacci decomposition

Fibonacci sequence is described as a number that starts with 0 or 1, and then followed by 1. Fibonacci which is also known as logical sequence is used in illustrating the decimal number of pixel values that are obtained by adding last two numbers. The aim of using the two previous numbers is to increase the robustness of the system. The security and robustness of the proposed scheme is enhanced by the use of Fibonacci decomposition. The Fibonacci is included in the image after the pixel value is converted from binary to Fibonacci

© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

decomposition. There are 8-bitplanes that make up the binary bitplane, and these 8 bits are occupied by the pixel value, thereby limiting the LSB in this situation. On the other hand, there are 12-bitplanes that make up the Fibonacci, and thus, facilitating efficient and flexible manipulation if the Fibonacci LSB [36]. The introduction of the conventional Fibonacci as made in the 13th century by Leonard of Pisa. The Fibonacci is defined using the following equation:

$$F(n) = F(n-1) + F(n-2)$$

Fibonacci has the following sequence [1,1,2,3,5,8,13,21,34,55,89,144,…,etc.]. This sequence allows the representation of numeric values as binary representation. The examples given below can be used in differentiating binary representation from Fibonacci representation:

N = 4
N = 8
Binary representation (1,2,4,8)
(1,2,4,8,16,32,64,128)
Fibonacci representation (1,1,2,3)
(1,1,2,3,5,8,13,21)

Special codes were introduced by Zeckendrof as a theorem for Fibonacci representation. According to this theorem, "each positive integer m can be represented as the sum of distinct numbers in the sequence of Fibonacci numbers using no two consecutive Fibonacci number" [37]. Rather than binary representation, the pixel value is represented using Fibonacci representation. When the conventional Fibonacci is used, all the values of pixel intensity are covered using 12 bits. For the application of Fibonacci to be made in steganography there are three key steps that are used, and they are given below:

- Change cover image pixel value into Fibonacci decomposition.
- Convert secret message into binary.
- Use LSB Fibonacci to substitute or embed the secret bits.

The extraction of secret message from stego-image involves applying the inverse procedure of embedding with tracking pixels (selected pixels for embedding).

From literature, there is an inability to exhibit high-quality stego-images from the available steganographic techniques and hence results in endangered image to human vision system. Moreover, it was perceived that some techniques enable plain direct data embedding into the image pixels, hence resulting in effortless data removal if the steganography formula is weakened. Accordingly, the concealed discrete data can be easily retrieved by the attackers, and thus, fail to be incorporated as genuine data in top-discrete security systems. Hence, the present research concentrates on according results to these difficulties by suggesting eight levels of security strategy.

3. PROPOSED SCHEME

This section provides a graphics description of the proposed scheme which is proposed in this study alongside its key modules. Through this graphic representation of the framework, the innovation of the framework is further explained so that the readers are able to have a clear image and deeper insight of the proposed scheme. The proposed scheme based steganography, is accompanied by eight layers of security for grayscale and colour images while different from other methods of steganography that are unable to provide a good level of security while maintaining the quality of image at a low cost and reasonable payload, in the sense that it is capable of maintaining balance among quality of image, security, payload and computational complexity. Figure 3 below presents a graphic description of the proposed scheme.

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

This scheme is made up of four major sub-stages which include: 1) the pixel selection preparation, involving the random selection of pixel based on diverse security layers. 2) Preparation of secret data, involving the compression and encryption of secret data prior to the embedding stage. 3) The third stage involves the adaptive hiding of chaotic secret data within cover images through the use of data embedding algorithm; this process enables the production of the stego images that can be transmitted to the concerned users. 4) Lastly, the use of extraction algorithm is employed in extracting the secret data from the stego image that has been delivered at the receiver terminal, afterwards, the data can be used accordingly. A brief description of these four major stages is given in the following sections .

3.1. Pixel Selection preparation

One of the rudiments of the embedding method is to identify the pixel required for hiding the secret message with high level of precision. It is not just enough to identify the embedment location, but it is also important to have knowledge of the subsequent location. Again, another important step is to find the complete trajectory so that the proposed algorithm cannot be tracked by anyone other than the receiver or communication partner. Bearing this in mind, the use of three-layer security together with two algorithms is employed in this framework so as to enhance the accomplishment of the goal of providing security with high level of precision in the selection of pixels. The pixel selection procedure is carried out using the Knight Tour (KT) algorithm and Henon Map Function (HMF) algorithm. With these algorithms, the cover image can be divided into blocks and sub-blocks until pixels have been obtained.

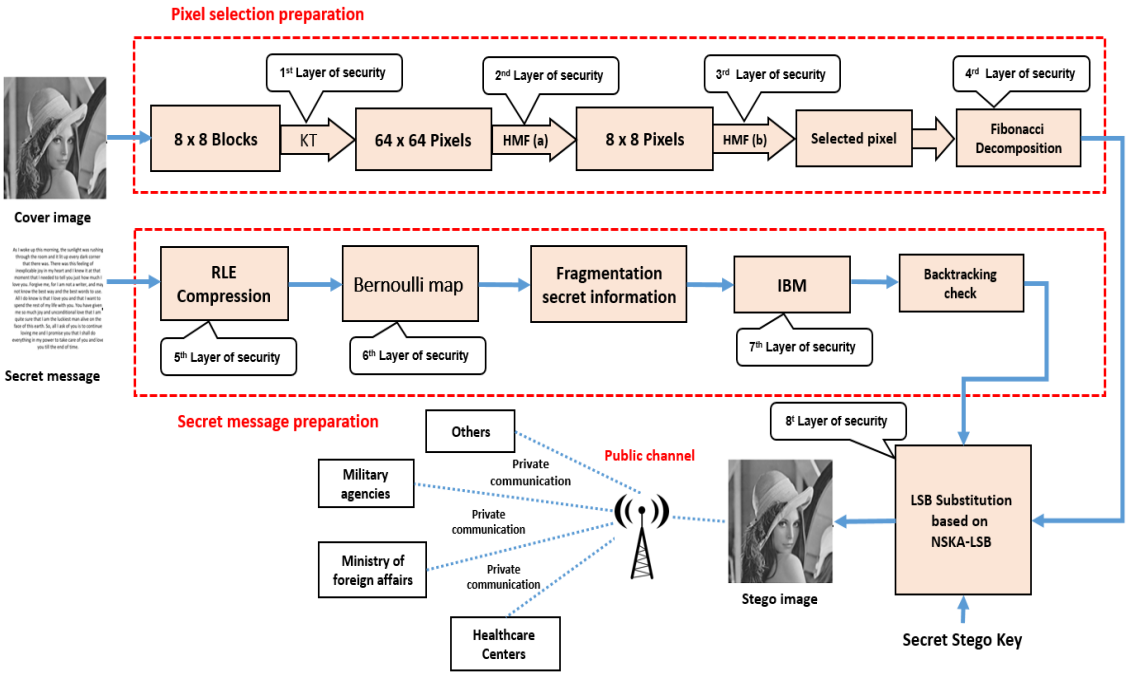

Figure. 3. Overall flow diagram of the proposed scheme

3.1.1. Knight Tour (KT) Process.

Generally, in Knight Tour, any square of the chessboard is used, and the visit to each square is paid just once [39]. Cover image is made up of (8 x 8) blocks, and each of them has (64 x 64) pixels, where the random selection of one block is made in every cycle. Afterwards, the primary cycle produces 63 blocks out of which one is used for the mapping the pixels in stego-key just once. For easy tracking, the blocks are labelled and positioned in the vector which is known as Knight Tour. With the use of this vector, the blocks are stored for use in subsequent processes. Once a block is selected, it is conveyed to Henon Map Function (HMF) stage. The first layer of security is achieved with this

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

random process. The main advantage of using KT algorithm is to maintain the proposed NSKA-LSB scheme robust against attacks. By choosing blocks of mixture between random and special formula the secrecy inside the cover image seems disappearing. In addition, it is impossible for the attacker to follow or guess if there is secret message in the image or not. Thus, it is worth using the KT in the proposed NSKA-LSB scheme to prepare block or pixel for the next stage of selecting the pixel.

3.1.2 Henon Map Function (HMF) Process

Henon map function alongside two random parameters are used in achieving the second and third layers of security. With normal random, the use of single parameter is employed in selecting the number; the initial condition for this function (single) is 10^{15} and probability of finding these numbers are 2^{50}. The complexity of random selection of the pixels can be increased by using two control values for the selection of the pixels for two stages, which are sub-block and pixel selection. An example of a dynamic system that demonstrates chaotic behaviour is the Henon map function. There are two control parameters possessed by the Henon classical function which include a=1.4 and b=0.3 as the chaotic function. This function is majorly dependent on a and b parameters, and this function can be depicted as coordinate point (X_n,Y_n) in the plane.

3.1.3. Fibonacci Decomposition with NSKA-LSB.

Fibonacci decomposition is used for the pixel that has been obtained. The fourth security layer is represented by this obtained pixel. In order to fortify the robustness and efficiency of data embedding, and enhanced NSKA-LSB Fibonacci technique is applied. As a result of binary representation, the cover image has 8-bitplanes. Therefore, through the application of Fibonacci decomposition, the bitplanes are changed to 12-bitplanes, which are more appropriate for the embedding process as they reduce the perceptibility of stego-image. In this paper, a new technique of handling LSB to check and embed as the need arises is proposed. The role of the presence of a statistical probability distribution for 1's and 0's in image is crucial in the proposed scheme. The distribution of 1's and 0's are checked through the selection of random image. Table 2 below presents balance or homogeneity of images.

Cover image (512 x 512)	Amount of pixels with zero value	0's %	Amount of pixels with one value	1's %
Lena	130,840	49.9	131,304	50.1
Peppers	127,698	48.7	134,446	51.3
Baboon	131,140	50.03	131,004	49.97
Lake	131,016	49.97	131,128	50.03

Table 2. Calculation of 0's % and 1's % for binary image in SSKA-LSB scheme.

The percentages which were obtained for binary image and bitplane (1) with homogenous distribution enabled easy detection by HVS. However, in small samples of image, the unorganized distribution can be explained by the increase in distribution. As a result of this, the imperceptibility of the system by attackers' bits was increased. For this limitation to be overcome, the image is partitioned into blocks and sub-blocks so that the disturbance can be facilitated. This made the system easy to track the embedded pixel. Another advantage associated with the use of Fibonacci sequence is the great difference in percentage 1's and 0's as presented in Table 3.

Table 3. Calculation of 0's % and 1's % for Fibonacci sequence in NSKA-LSB scheme.

Cover image (512 x 512)	Amount of pixels with zero value	0's (%)	Amount of pixels with one value	1's (%)
Lena	161,724	61.69	100,420	38.31
Peppers	157,392	60.04	104,752	39.06
Baboon	161,965	61.78	100,179	38.22
Lake	161,844	61.74	100,300	38.26

As a result of the increased disturbance, the secrete message is embedded under this condition. A comparison of the secret message bits with LSB is done so as to determine if the amount of identical bits are greater than the non-matching bits. Afterwards, the secret message is reversed and embedded , or a direct insertion of the secret message using IBM . This in turn maintains the maximum disturbance, and the probability of detection by one attacker is avoided by maintaining this maximum disturbance. The implication of this is that as the amount of data increases, data distribution stability improves.

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

3.2 Secret Message Preparation.

There are two main stages that secret message passes through, and they are compression and encryption. After the message is compressed, then it is goes through the next stage which is the stage of encryption. The use of alphabetical letters is employed in randomly generating the secret messages in diverse lengths.

3.2.1. Run-Length Encoding (RLE).

In the proposed method, one of the widely used compression technique is used in compressing the text before it is embedded; the technique is known as Run-Length Encoding (RLE). The main idea behind using the RLE is to minimize the redundant letters by encoding the letter repeated d of n times to become (n (d)). This implies that d letters in the text are repeated n times. The use of the RLE technique is essential when the bytes of more redundant values are to be compressed. More so, the role of this algorithm becomes more dominant if there is repetition in the file. In some cases, the use of this algorithm is employed in compressing the text. In addition, the use of this method is also employed in text, especially with the presence of more space. The working of this algorithm can best be explained using an example which is given as follows:
Consider the text as the following characters:

R T A A A A S D E E E E E

The RLE can be represented as follows:

R T *4A S D * 5 E

The manner in which the redundant character is reduced is shown in this example, and this is known as run. The fifth layer of security is achieved in the proposed scheme. RLE technique offers one great benefit which is adaptability of the algorithm to different sorts of files which include text (pdf or txt) and image formats.

3.2.2. Bernoulli's map (BM).

This section presents an explanation on Bernoulli's map, which is used together with the proposed NSKA-LSB scheme. The encrypted cipher text of the secret message is produced through the use of the Bernoulli's map. The key which is used for the encryption of secret data in chaotic system is known as the chaotic sequence. With the aid of the chaotic map, the key which used in the creation of a chaotic sequence is produced [11]. With this algorithm, the sixth security layer of the proposed scheme is achieved. The key steps involved in the Bernoulli's map mechanism, which are included in the proposed framework are presented in Algorithm 1.

Algorithm1: Bernoulli's map Algorithm

Input: Secret Message (M).

Generate a chaotic sequence

$$Z_{t+1} = \mu(1 - Z_t)$$

$$Z_t \in (0,1), \mu \in (1,4), \quad t = 0,1,2,\ldots$$

Assuming the random sequence given in the formula above formula is:

$$Z = [Z_t \mid 0 \leq Z_t \leq 1] \quad t = 0,1,2\ldots$$

Use the binary formula to produce a binary sequence

$$Q(t) = F(Z_t) = \begin{cases} 0 & 0 \leq Z \leq 0.5 \\ 1 & 0.5 \leq Z \leq 1 \end{cases} \quad \text{Where } t = 1,2,3,4,\ldots$$

Convert the secret information to binary equivalent

$$M = (m_1, m_2, m_3, \ldots, m_n)$$

Use the following to encrypt the secret information:

$$E = \{E_i \mid E_i = (Q_t \otimes M_i) \oplus M_i\}, \quad t = 0,1,2,\ldots$$

Output: Encrypt secret information M^{ESI}

3.2.3. Inverting Bit Map IBM.

In the proposed scheme, subsequent to the selection of the pixels, they are organized into a sub window of 8 x 8 pixels. Afterwards, each pixel's LSB is used to obtain (64 bits), which will now be ready for embedding. At this point, there are 64 bits obtained from the image, and these 64 bits will be substituted with 64 bits from the secret message. More so, at this stage the use of the inverting bit map IBM is employed in checking the correspondence between the bits inside the original image and the secret message bits. In an event that the number of corresponding bits is less than that of the mismatched bits, then the secret message is inverted and embedded, if not, secret bits should be embedded directly.

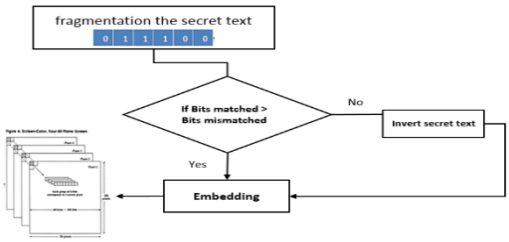

Figure. 4. Inversing bit map process

The seventh security layer is achieved using the IBM. The embedding algorithm and IBM

Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mechanism that is incorporated in the proposed scheme is illustrated in Figure 4.

3.3. Embedding process

It is the responsibility of the embedding algorithm to hide the secrete message within a cover image. The embedding algorithm is able to conceal the encrypted message within the LSB layer adaptively with the aid of the stego key. In algorithm 1, the key steps involved in the proposed embedding mechanism are illustrated.

ALgorithm2: Embedding Algorithm

Input: Cover image (I^c), Stego key (K^s), Secret Message (M).

1. Initialize I^c = Cover Image , M = Secret Message , K^s = Stego key
2. Apply RLE algorithm on M to get the compression bit stream (M^{cms})
3. Apply BM using algorithm1on M^{cms} to get encrypt secret information (M^{esi})
4. Let L = length of M^{esi}
5. Segment the M^{esi} into groups each with 64 bits.
6. Select an appropriate cover image I^c from dataset of cover images (DS^{ci})
7. Generate random number 1 and arrange it according to KT vector
8. Select one block of (8 x 8) blocks via KT vector
9. Generate random number 2 and arrange it according to HMF -a vector
10. Select one sub-block of (64 x 64) pixels via HMF-a vector
11. Generate random number 3 and arrange it according to HMF -b vector
12. Select the destination pixel via HMF-b vector
13. Apply the Fibonacci Decomposition to destination pixel before embedding
13. Generate EM vector and arrange it according to Odd/Even
14. Mark the LSB of each pixel and M^{esi} group
15. If Bit matched > Bit mismatched then
    Embed directly from secret to pixel using step 17
    Else
    Invert the secret message then embed using step 17
16. Loop from I=1 : N
17. Get M^{esi} bit (0 or 1)
    a. If M^{esi}=0 and pixel is even, Do no change in 1-LSB layer.
    b. If M^{esi}=0 and pixel is odd, Do Change in 2-LSB layer via replace 0 to LSB layer.
       Else if 2-LSB layer is full, Do Change in 1-LSB layer.
    c. If M^{esi}=1 and pixel is odd, Do no change in 1-LSB layer.
    d. If M^{esi}=1 and pixel is even, Do change in 2-LSB layer via replace 1 to LSB layer.
       Else if 2-LSB layer is full, Do Change in 1-LSB layer.
18. I=I+1
19. Repeat Step 16 until all the secret bits are embedded, and the stego image is obtained.

Output: Stego Image (I^s)

A clearer picture of the central idea of the proposed embedding algorithm is presented in the procedure shown in Figures 3. Let P be a cover image with pixels [P1, P2, P3, P4] as binary and encrypted secret message bits using algorithm 1 , M^{ESI} = (00110001)2. For the avoidance of confusion, some of the intermediate steps are skipped, and more attention is paid to the central idea.

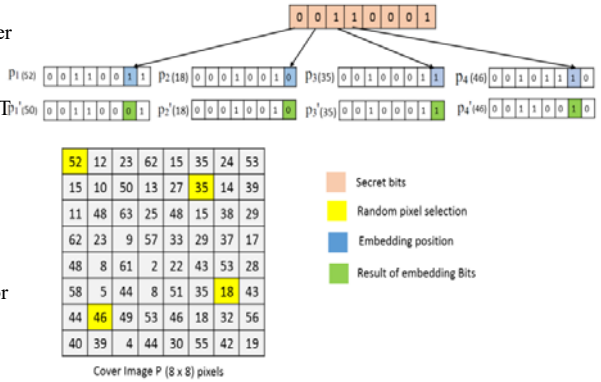

Figure 5. Examples of embedding for the proposed scheme

3.4. Extraction process.

Extracting process aims in getting data from the LSB pixels and needs to precede the process postulated and built within the embedment procedure. It is situated in the other receiver, which comprises guideline with the agreement between two parties through stego-key to direct the processes. The extracting procedure is identical to the embedment but in an opposite form, this implies that the LSB components of pixels evaluate pixel.

Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. RESULT AND DISCUSSIONS

In the results performed in this study, the use of MATLAB tool alongside eight standard grayscale images that are contained in Figure 6 was employed. The images with size (512 x 512) were obtained from USC-SIPI image database. The results are obtained considering the full capacity of each image for the respective techniques. The different stego-images for the proposed technique with embedding percentage (EP) = 1.5 are contained in Figure 7. The proposed approach has been evaluated using parameters such as PSNR, EC, bits per pixel (BPP) and Structural Similarity Index (SSIM).

Figure 6 .Cover Images Used In The Proposed Scheme

3.1. Analysis Based on EC, PSNR, BPP and SSIM

The embedding capacity EC is defined as ratio of the number of message bits to the number of cover pixels [2]. This is directly related with the number of pixels used in the scheme that is proposed in this study.

$$C = \frac{\text{The number of message bits}}{\text{The number of cover images's pixels}} \quad (2)$$

In the current study, diverse payload capacities were used, and presented as a percentage so as to be in accordance with that of recent studies in this field. For more clarification the following is given:

- 16384 Bytes which is equal to 6.25% for a given image 512 x 512, meaning that every two pixels = 16 bits, so 1/16 = 6.25% when 1 bit of two pixels is embedded.
- 32768 Byte which is equal to 12.5% for a given image 512 x 512, meaning that every pixel = 8 bits, so 1/8 = 12.5% when 1 bit of one pixel is embedded.
- 49152 Byte which is equal to 18.75% for a given image 512 x 512, meaning that every two pixels = 16 bits, so 3/16 = 18.75% when 1.5 bit of one pixel is embedded.

The reason these percentages are used in this study is that diverse payloads were used in previous studies, and we need to have uniform tools so that we can obtain fair results.

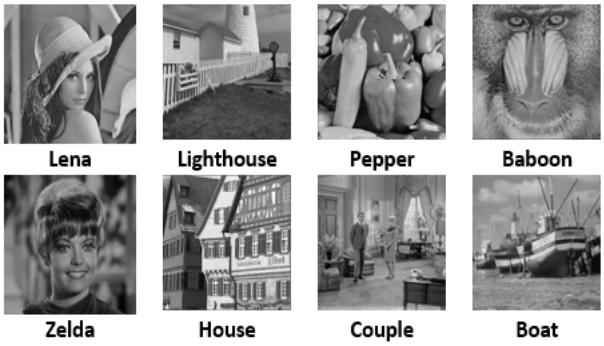

Figure 7. Stego-images for the proposed scheme for EP = 18.75%.

The method for image quality evaluation is determined by peak signal to noise ratio (PSNR), which is calculated after the process of embedding to compare between original and stego images. The process of embedding data is considered to be imperceptible to the human vision system (HVS), if the result of PSNR calculation is equal or greater than 30db [4] .By applying the following equations PSNR can be calculated.

$$PSNR = 10log_{10}\left(\frac{255}{MSR}\right) \quad (3)$$

Where ,MSE is mean square error, which is calculated by the following equation :

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij}) \quad (4)$$

Where, m and n are the images' sizes while x and y are the cover and stego images respectively. By applying the PSNR measures which mentioned above , the fidelity of the stego image is evaluated against the original carrier image. [1] In other words, the level of distortion in the stego image is measured against the carrier image; this is measured in decibel (dB). In measuring the similarity between the original image and the stego-image, the use SSIM is utilized [2]. Eq. (16) is used in computing the similarity. The range of SSIM value is from - 1 to 1. If the SSIM value is 1, it means that there is no difference between the original image and the stego-image.

$$SSIM = \frac{(2P_O Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2 Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2)} \quad (5)$$

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

For the original image and the stego-image, they represent the mean pixel value, variance, and standard deviation respectively. rOS represents the covariance between the original image and the stego-image while the constant c1 = k1L and c2 = k2L. For the grayscale image, k1 = 0.01, k2 = 0.03, and L = 255.

Table 4. Results For Proposed Scheme With 6.25% Of Ep

Cover image 512 x 512	Proposed Scheme (6.25%)					
	PSNR	EC	Bpp	SSIM	BER	BER-P
Lena	72.30	131,072	0.5	1	0.01383	1.38%
Lighthouse	72.10	131,072	0.5	1	0.01386	1.38%
Pepper	72.44	131,072	0.5	1	0.01380	1.38%
Baboon	72.35	131,072	0.5	1	0.01382	1.38%
Average	**72.29**	**131,072**	**0.5**	**1**	**0.01382**	**1.38%**

Table 5. RESULTS FOR PROPOSED SCHEME WITH 12.5% OF EP

Cover image 512 x 512	Proposed Scheme (12.5%)					
	PSNR	EC	Bpp	SSIM	BER	BER-P
Lena	66.63	265,144	1	0.99	0.01500	1.50%
Lighthouse	66.46	265,144	1	0.99	0.01504	1.50%
Pepper	66.70	265,144	1	0.99	0.01499	1.49%
Baboon	66.56	265,144	1	0.99	0.01502	1.50%
Average	**66.58**	**265,144**	**1**	**0.99**	**0.01488**	**1.48%**

Table 6. RESULTS FOR PROPOSED SCHEME WITH 18.75% OF EP

Cover image 512 x 512	Proposed Scheme (18.75%)					
	PSNR	EC	Bpp	SSIM	BER	BER-P
Lena	61.10	393,216	1.5	0.99	0.01633	1.63%
Lighthouse	61.06	393,216	1.5	0.99	0.01634	1.63%
Pepper	61.22	393,216	1.5	0.98	0.01631	1.63%
Baboon	61.20	393,216	1.5	0.99	0.01632	1.63%
Average	**61.14**	**393,216**	**1.5**	**0.99**	**0.01632**	**1.63%**

3.2. Robustness Evaluation against Bit Error Rate (BER).

The robustness of the proposed scheme was evaluated using bit error rate (BER). Robustness refers to the ability of the secret bits to resist attacks. The value of PSNR is inverted so as to obtain the bit error rate using the following equation:

$$BER = \frac{1}{PSNR} \quad (6)$$

The portion of the original cover image's qubits that is converted during the process of steganography is determined by the BER. In the case whereby the PSNR is 50 db, the BER would be 0.02, i.e., alterations have been made to 2% BER-P of bits during the process. Tables 4,5 and 6 present the results of the calculated BER ,PSNR, EC, SSIM, BER-P and Bpp in the simulation of the current study.

5. CONCLUSION

As sensitive information is increasingly being transmitted over public network, the security of such sensitive information has become a challenge and an interesting area of research in the past decades. So, the current study suggests a secure image steganography scheme which is known as a new stego key adaptive LSB (NSKA-LSB) scheme, which depends on four stages for the provision of better data-hiding algorithm in cover images by the volume, image quality, and security. In this paper a new adaptive of least significant bit substitution technique, merging two random functions, and chaotic technique. The incorporation of the adaptive LSB substitution technique is incorporated in embedding the secret information within the carrier image, with respect to the stego key. The amalgamation of two random function exhibits system worthiness against any tracker trying to disclose the pixel to embed at the start or the pixels succession. The secret message is passed through two main stages , they are compression and encryption. The main idea behind using the compression is to minimize the redundant letters by encoding the letter repeated d of n times to become (n (d)), this done by using RLE technique. The encrypted cipher text of the secret message is produced through the use of the Bernoulli's chaotic map before embedding. The suggested technique entails direct or inverse embedding of secret bits strengthening the complexity and invisibility of the embedding activity. This formula is deliverin eight levels of security incorporated together to elevate shielding from attacks. The results of the experiment revealed that the algorithm has better image quality index, peak signal-to-noise ratio, and payload used in the evaluation of stego image.

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

REFERENCES:

[1] Hashim, Mohammed, Et Al. "A Review And Open Issues Of Multifarious Image Steganography Techniques In Spatial Domain." *Journal Of Theoretical & Applied Information Technology* 96.4 (2018).

[2] Hashim, Mohammed Mahdi, Et Al. "Performance Evaluation Measurement Of Image Steganography Techniques With Analysis Of Lsb Based On Variation Image Formats." *International Journal Of Engineering & Technology* 7.4 (2018): 3505-3514.

[3] Domain, W. T. I. S. "A Review And Open Issues Of Diverse Text Watermarking Techniques In Spatial Domain." *Journal Of Theoretical And Applied Information Technology* 96.17 (2018).

[4] Mahdi Hashim, M. O. H. A. M. M. E. D., Mohd Rahim, And Mohd Shafry. "Image Steganography Based On Odd/Even Pixels Distribution Scheme And Two Parameters Random Function." *Journal Of Theoretical & Applied Information Technology* 95.22 (2017).

[5] Hashim, Mohammed Mahdi, Et Al. "An Extensive Analysis And Conduct Comparative Based On Statistical Attach Of Lsb Substitution And Lsb Matching." *International Journal Of Engineering & Technology* 7.4 (2018): 4008-4023.

[6] Mahdi, Mohammed Hashim, Et Al. "Improvement Of Image Steganography Scheme Based On Lsb Value With Two Control Random Parameters And Multi-Level Encryption." *Iop Conference Series: Materials Science And Engineering*. Vol. 518. No. 5. Iop Publishing, 2019.

[7] Taha, Mustafa Sabah, Et Al. "Combination Of Steganography And Cryptography: A Short Survey." *Iop Conference Series: Materials Science And Engineering*. Vol. 518. No. 5. Iop Publishing, 2019.

[8] Mahdi Hashim, M. O. H. A. M. M. E. D., Mohd Rahim, And Mohd Shafry. "Image Steganography Based On Odd/Even Pixels Distribution Scheme And Two Parameters Random Function." *Journal Of Theoretical & Applied Information Technology* 95.22 (2017).

[9] 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.

[10] Sahu, Aditya Kumar, Gandharba Swain, And E. Suresh Babu. "Digital Image Steganography Using Bit Flipping." *Cybernetics And Information Technologies* 18.1 (2018): 69-80.

[11] Yeung, Yuileong, Et Al. "Secure Binary Image Steganography Based On Ltp Distortion Minimization." *Multimedia Tools And Applications* (2019): 1-22.

[12] Sahu, Aditya Kumar, And Gandharba Swain. "A Novel N-Rightmost Bit Replacement Image Steganography Technique." *3d Research* 10.1 (2019): 2.

[13] Taha, Mustafa Sabah, Et Al. "Wireless Body Area Network Revisited." *International Journal Of Engineering & Technology* 7.4 (2018): 3494-3504.

[14] Saad, Mohammed Ayad, S. T. Mustafa, Mohammed Hussein Ali, M. M. Hashim, Mahamod Bin Ismail, And Adnan H. Ali. "Spectrum Sensing And Energy Detection In Cognitive Networks." *Indonesian Journal Of Electrical Engineering And Computer Science* 17, No. 1 (2019): 465-472.

[15] Liu, Wanteng, Xiaolin Yin, Wei Lu, Junhong Zhang, Jinhua Zeng, Shaopei Shi, And Mingzhi Mao. "Secure Halftone Image Steganography With Minimizing The Distortion On Pair Swapping." *Signal Processing* 167 (2020): 107287.

[16] Luo, Weiqi, Fangjun Huang, And Jiwu Huang. "Edge Adaptive Image Steganography Based On Lsb Matching Revisited." Ieee Transactions On Information Forensics And Security 5, No. 2 (2010): 201-214.

[17] Li, Bin, Ming Wang, Xiaolong Li, Shunquan Tan, And Jiwu Huang. "A Strategy Of Clustering Modification Directions In Spatial Image Steganography." Ieee Transactions On Information Forensics And Security 10, No. 9 (2015): 1905-1917.

[18] Mielikainen, Jarno. "Lsb Matching Revisited." Ieee Signal Processing Letters 13, No. 5 (2006): 285-287.

[19] Subhedar, Mansi S., And Vijay H. Mankar. "Secure Image Steganography Using Framelet Transform And Bidiagonal Svd." *Multimedia Tools And Applications* (2019): 1-22.

[20] Yahya, Abid. "Introduction To Steganography." In *Steganography Techniques For Digital Images*, Pp. 1-7. Springer, Cham, 2019.

[21] Sun, Shuliang. "A Novel Edge Based Image Steganography With 2k Correction And

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

Huffman Encoding." *Information Processing Letters* 116, No. 2 (2016): 93-99.

[22] Singh, Amit Kumar, Mayank Dave, And Anand Mohan. "Hybrid Technique For Robust And Imperceptible Multiple Watermarking Using Medical Images." Multimedia Tools And Applications 75, No. 14 (2016): 8381-8401.

[23] Liao, Xin, Sujing Guo, Jiaojiao Yin, Huan Wang, Xiong Li, And Arun Kumar Sangaiah. "New Cubic Reference Table Based Image Steganography." *Multimedia Tools And Applications* 77, No. 8 (2018): 10033-10050.

[24] Muhammad, Khan, Jamil Ahmad, Haleem Farman, And Zahoor Jan. "A New Image Steganographic Technique Using Pattern Based Bits Shuffling And Magic Lsb For Grayscale Images." *Arxiv Preprint Arxiv:1601.01386* (2016).

[25] Sahu, Aditya Kumar, Gandharba Swain, And E. Suresh Babu. "Digital Image Steganography Using Bit Flipping." Cybernetics And Information Technologies 18, No. 1 (2018): 69-80.

[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 (2015): 228.

[27] Jain, Aman. "A Secured Steganography Technique For Hiding Multiple Images In An Image Using Least Significant Bit Algorithm And Arnold Transformation." In *International Conference On Intelligent Data Communication Technologies And Internet Of Things*, Pp. 373-380. Springer, Cham, 2019.

[28] Zhang, Xiang, Fei Peng, And Min Long. "Robust Coverless Image Steganography Based On Dct And Lda Topic Classification." *Ieee Transactions On Multimedia* 20, No. 12 (2018): 3223-3238.

[29] Tresor, Lisungu Oteko, And Mbuyu Sumbwanyambe. "A Selective Image Encryption Scheme Based On 2d Dwt, Henon Map And 4d Qi Hyper-Chaos." *Ieee Access* 7 (2019): 103463-103472.

[30] 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 (2015): 228.

[31] 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.

[32] 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.

[33] 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.

[34] Kuo, Wen-Chung, Et Al. "Secure Multi-Group Data Hiding Based On Gemd Map." Multimedia Tools And Applications 76.2 (2017): 1901-1919.

[35] Valandar, Milad Yousefi, Milad Jafari Barani, Peyman Ayubi, And Maryam Aghazadeh. "An Integer Wavelet Transform Image Steganography Method Based On 3d Sine Chaotic Map." *Multimedia Tools And Applications* 78, No. 8 (2019): 9971-9989.

[36] Nikam, Virendra P., And Shital S. Dhande. "Extended Fibonacci Series For Selection Of Carrier Samples In Data Hiding And Extraction." In *International Conference On Intelligent Data Communication Technologies And Internet Of Things*, Pp. 40-50. Springer, Cham, 2019.

[37] Ahmed, Mohamed Sherif. "Stegocrypt: Fibonacci And Rudin–Shapiro Sequence–Based Bit–Cycling And Aes." (2019).