Journal of Theoretical and Applied Information Technology
15th August 2019. Vol.97. No 15

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

DIGITAL IMAGE STEGANOGRAPHY SCHEME BASED ON SK-LSB SUBSTITUTION AND THREE PARAMETERS ENCRYPTION METHOD

[1]MOHANAD NAJM ABDULWAHED
[1]Materials department, University of Technology, Baghdad, Iraq
E-mail: mohanadnajmabdulwahed@gmail.com

ABSTRACT

Recently, steganography has played an important part in the field of communication, especially in image steganography. The major points of image steganography are the image quality (imperceptibility) of the stego image and the security of the system towards stopping the recoverability of the secret data. Several digital image steganography methods has been introduced, all are focused based payload and image quality. Moreover, there is a trade-off amidst these two metrics and saving a better balance amidst them is yet a challenging case. Therefore, previous methods fail to realize a high security level because to direct embedding secret information inside image without cryptography consideration, making information extraction relatively simple for adversaries. So, a new steganography scheme based on two control random parameters and new encryption method based on three parameters can address the security challenge while new stego key-LSB substitution, SK-LSB can ensure the imperceptibility of the stego image. The objectives of paper to increase the security and PSNR of the stego image. The Hyper technique has been used to compress the secret information prior to embedding, this will also ensure an increase in the payload capacity. The proposed scheme takes effect after compressing and encrypting the secret information. This algorithm is provide different layers of security worked together to augment protection from attacks. The experimental results shows the efficient scheme from PSNR, SSIM and payload for evaluating the stego image compared to the existing methods.

Keywords: *Steganography,* Cryptography*, SK-LSB substitution, PSNR, SSIM, BER.*

1. INTRODUCTION

Network revolution has made digital communication easy and has resulted in a remarkable increase in the number of active digital communication users. Mmeanwhile, it comes with security challenges with respect to data transmission over a public network. In order to secure data, two major processes (digital watermarking and steganography) have been used. Digital watermarking is an early technique created for secure personal information transmission, and various methods have been proposed in this field to ensure the privacy of messages [3]. Steganography refers to the science converting a message into a form that ensures a complete undetectability of any hidden piece of information in the carrier. Steganography ensures that a secret information is kept undetectable by the human visual system (HVS) [2].

Secure and Pure Communications are widely utilized in almost all areas. The main benefits are medical, military, multimedia and industry, in which radio communications can be used for internal and external security purposes. In the medical field, key private information is hidden in the medical information itself, followed by DNA and dispersed. This will help prevent leakage of private information in unauthorized hands. Steganographic systems are more reversible because the cover and hidden data must be extracted separately on the receiver side. Security is a major concern in military and military communications. Open channels may be compromised and legitimate communication is much more important. These stegano systems use multi-layer encryption techniques before the embedding process. In industry and corporate communications, credibility and security are critical because insecure communications may cause serious data leakage.

The word of *steganography* originates from ***Greek*** term that means as a *protected* writing. It is regarded as a unique area of data concealment, also *considered* as an art of science for transmission that is not visible. The aim of making the communication invisible is to hide a secret information in a cover image (CI), thereby enhancing its imperceptibility; the existence of the secret information (SI) is often recognized by just the sender's and receiver's [4]. *The* steganography elements, basically included an information, cover object, a stego key for improved security and embedding mechanism. The carrier object in which the secret information (SI) is hidden in could be a video, an audio, text or image [71]. The use of steganography can be employed in a broad spectrum of applications like the safe distribution of secret data in intelligence agencies and military, improvement of mobile banking security, coversion of communication between two communicating entities and online voting system [5]. The application of steganography can be of great benefits, however, it can be quiet risky because it can be used by hackers for sending Trojans and viruses to compromise sensitive systems. More so, the use of this technology can be employed in the exchange of secret information by criminals and terrorists [6]. Researches have continued to make efforts towards developing schemes that make detection process complex, and to a lesser range the extraction, of the concealment information. This is the security side which authors endeavor to *improve*. Nevertheless, the only area that needs to be improved upon is security. Some other problems include capacity of hiding, quality of stego, stego system robustness.

Quality of stego means the aspect that Is mostly associated with security, and thus it is of great importance for steganography schemes to be developed so as to protect the secret data. Stego quality is largely associated with the eavesdropper's inability to know the difference among the stego media (SM) and the cover media (CM) because of the *amount of* noise in the stego media (SM). A SM of less quality reduces a scheme's security, thereby providing clues about the existence of a confidential message. On the other hand, robustness is characterized as the strength of the SM to repel attacks irrespective of if the attacks are capable of destroying the secret data or not. Capacity is defined as the amount of information that can be hidden within the CM relative to the alteration in the quality of stego image (SI). The capacity of digital images is measured in bit-per-pixel (*bpp*). [7, 8, 9].

The correlation between hiding payload capacity (PC) and quality of stego media SM is purely described via a balance which authors attempt to achieve. Most often, the quality of stego medium is reduced by concealment of huge amounts of data within a cover medium. Consequently, hiding capacities have continued to remain comparatively low because of this negative effect on the quality of stego [10, 11].

With respect to mechanism of embedding, the techniques of steganography are partitioned to two major *categories*, which are spatial domain (SD) and transform domain (TD). The SD involve the direct modification of pixels with larger embedding capability and less depletion of image quality. These images are low in robustness due to the impossibility of totally recovering the embedded data if the stego images have been ***exposed*** to modification of the attacks such as crop, compress, filtering or rotation. An example of Spatial Domain (SD) technigue is the LSB replacement or called "substitution" methods [12, 13, 14], pixel-value-differencing methods [15, 16], gray-level –modification (GLM) methods [17, 18], Edges *based* methods [17, 18, 19] and pixel-pair-matching method [21].

On the other hand, the transform domain (TD) techniques involve hiding a message using transformed coefficients, which in turn reduces the vulnerability of the message to various kinds of attack [72]. Some of the methods that fall under this characters are include Discrete-Wavelength-Transform (DWT) methods [22], Discrete-Fourier-*Transform* (DFT) method [23], Integer-Contour-Transform (ICT) method [24], and Discrete-Cosine-Transform (DCT) method [25]. The existing meth*o*ds under the transform domain are regarded better than those under spatial because of their robustness, which in turn enhances their suitability for water*marking* like copyright-protection (CP) [26]. Nevertheless, these methods are accompanied by limitations such as lower payload, high level of computational complexity. More so, they are unable to provide a balance among image quality IQ, Payload and Security. Thus, it is based on the spatial domain that the framework provided in this study is developed, giving consideration to spatial domain (SD) techniques.

Recently, authors have proposed different kinds of steganography methods within the spatial domain, and one of such methods is referred to as Least-*Significant*-Bit (LSB) replacement. The use of this scheme involves replacing the host image with a message. However, with this scheme, detection is relatively easy when steganalysis is used, and this is

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

because of the uneven modification of pixel and simplicity [26]. LSB-matching scheme is used to add or subtract a numerical 1 into the pixels of a Cover-Image (CI) based on a secret *data* within an aim of reducing the aforementioned limitation [12]. This way, the possibility of detecting a message is reduced, but with distortion of marked images. A modification of the LSBM scheme was made and called LSBM revisited (LSBMR) [12]. Here, the relation between a pair of pixels is regarded as a way of concealing two bits simultaneously, and thus, reducing a *distortion* rate of marked images 0.325 for 0.5 bpp or 6.25% EP. As a way of further reducing the marked images detectability, the LSBMR was combined with edge-based hiding mechanism by Luo et al. [28]. These researchers adaptively selected regions of a cover image for concealing message according to the need. Despite the fact that these schemes offer some benefits, they are prone to problems such as: a) directly embedding sensitive information in the host image with encryption, which in turn facilitates the operation of attackers in terms of easy secret message extraction by cracking the embedding algorithm, b) stego images can be visually altered due to the usage of ineffective embedding algorithms, thereby increasing the possibility of detection by HVS, and c) imbalance between quality of image, payload, computational complexity and security, which in turn makes them unsuitable for use in Real-Time RT and Top-Secret TS *security* applications. To overcome these problems a new image steganography scheme has been proposed based on new encryption method.

The real motivation behind steganography is the data sharing in an undetectable manner with keep the visual quality of cover image high as possible. The main motivation of the scheme is to secure steganography scheme which combines the benefits of cryptography method and steganography with the aim of achieving the better security , and to reduce the modification per pixel value which indirectly increases the visual quality of stego-image by using a new scheme. This paper makes the following key contributions.

1. Propose a secure steganography scheme which combines the benefits of cryptography method and steganography with the aim of achieving the better quality of image, payload and security, thus, enhancing the suitability of the proposed scheme for use in security applications (SA).

2. A new encryption method based on three parameters (to increase complexity) has been used before the process of data embedding to encrypt 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.

3. To locating the random pixel for embedding secret information, the Henon map function with three parameter has been used to makes the system worthy against any tracker trying to reveal which pixel to embed first or the pixels sequence.

4. The embedding of the secret information is done in a random region within an image through the use of a novel stego key -LSB substitution (SK-LSB). This way, the visual quality (VQ) of the stego images (SI) is enhanced while the extraction of data is made difficult, thereby reducing the detectability by HVS. The structure of the paper is rebuild as following sections: In section 2, introduced briefly description about the simple steganography method that are related to the proposed work. The proposed scheme describes in section 3. In Section 4, Experimental result is given in details. Finally, in section 5, the conclusion of this paper.

2. RELATED WORK.

Least Significant Bit (LSB) substitution is *a* conventional and simple method used to insert secret information within a cover image [29]. 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 range from **0 to 255** and the bit depth for 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 for 24 bits, the carrier object is initially partitioned to 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 (SI). 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. Eembedding percentage (EP) of LSB which include 6.25% and 12.5% which means 0.5 and 1.0, bpp

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

respectively are used based on the capacity that is to be embedded. Being that a special form of the LSB-substitution scheme is utilised in the proposed scheme in this work, it is therefore mathematically expressed with enough detail to enhance it a better understanding of the basic concept in section 3. The basic concept of the LSB-based steganography is further elucidated utilizing a simple instance. Assume that lena image is a cover image , selected 8 random pixels with their decimal and binary values as given in figure 1. (A) Is a letter that represented as a secret information.

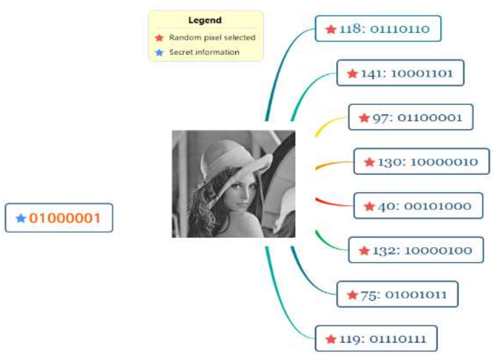

Figure 1. Binary representations and secret later before embedding

Let X be the secret information, such that X= 'A' with the binary form X= 01000001. To embed X inside a given cover image, the LSB of the pixels [P=P_1, P_2, P_3,....... P_8] are replaced with the bits of X (01000001) and the resulting pixel after the embedment is represented as [P ′ = P1 ′ , P2 ′ , P3 ′ , ... P8 ′]. with their decimal and associated binary values as given in figure 2. The embedding scheme is utilized to conceal the bits *of the secret* text to *LSB* of randomly selected *pixels***.** The pixel is selected based on the stego key that the sender shared with the recipient [30]. This technique can be easily implemented and can ensure the security of the hidden information.

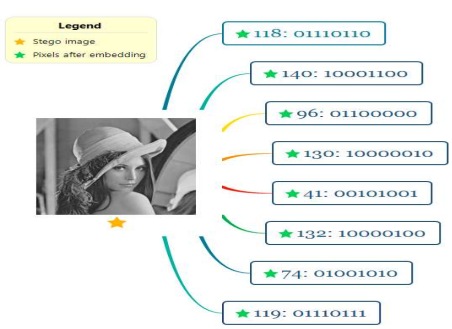

Figure 2. Binary representations after embedding

Wu, et al. [32] suggested a novel noise-based steganography system for secret data embedding. The system depends on noise to confer security against statistical attacks and to increase embedding capacity. Sedighi, et al. [33] demonstrated the effected of choosing the cover image (CI) in advance on the capacity and security of steganography systems. Mohamed and Mohamed [31] opined that the capacity of a steganography system depends on the method used. The studies on the improvement of the embedding method based on the image edge area are still preliminary but promising [32].

An imperceptible image steganographic method which is based on the PBSA and M -LSB ,proposed by Muhammad et al. [34]. Here, the secret data is altered through encrypted and then, shuffled using a pattern-based bit shuffling algorithm (PBSA). Later, the M - LSB method is deployed to embed the encrypted message by scattering the secret message inside the image pixel. This makes the extraction of the hidden message more difficult for the attackers. The proposed scheme in this work is evaluated qualitatively and quantitatively to verify its effectiveness.

A method of secure image steganography based on the SKA-LSBs scheme alongside multi-level cryptography was proposed [15]. In their proposal the first step involve the use of the TLEA to encrypt the stego key. Afterwards, the use of the MLEA is employed in encrypting a Secret information prior to its concealment in an image through the use of an adaptive LSB-Substitution Scheme with the aid of a stego key (SK) [35].

Khamy et al. have proposed a new steganography method to reduce and solve the distortion on the stego –image (SI). The proposed scheme uses two LSB *steganography algorithms* based NEQR. The cover image (CI) is divided to blocks and each block concealment one secret bit. Firstly, LSB algorithm, the secret bit is embedded by directly replacing the LSB bits of the cover image with the secret message bits, and then, the second LSB algorithm is a block LSB which embeds a secret bit into a *number of pixels that belong to one* image block [36].

A three-phase intelligent method for color images has also been proposed for the improvement of the embedding payload and visual imperceptibility [37]. Prior to the embedding step in this method, a

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

learning system (LS) is first applied, while the remaining the phases are applied post the embedding process. The number of embeddable secret bits inside the pixels is determined using an ANN and an adaptive GA. From the results, the proposed system successfully embedded a larger payload of up to 12 bpp with achieved a good visual quality.

A novel secure steganography method was put forward by [38] which was based on edge detection and Huffman Encoding. Coherent bit length was also adopted to embed different bits of secret data according to the values of the edge pixels values.
Singh et al [30] proposed a spatial domain-based color image steganography technique which is dependent on the hash function and edge detection technique. In this method, the canny edge is first applied on the color image to detect the edges before using the hash function algorithm to embed the secret text into the image. Different image formats such as -jpg, jpeg, bmp, tiff, etc can be used in the proposed scheme.

Three levels of security is explained by a new scheme to hide secret message into a color Image. First layer, Advanced Encryption Standard (AES) algorithm is used to encrypt the secret message by accepting a 128-bit secret key. Generating number of segments with different dimensions of an input cover image by accepting the same secret key by using NUBASI algorithm and this is the second layer. Last layer of security is by embedding the secret message into the segmented image by using Randomized Secret Sharing (RSS) algorithm [39].

Sahib Khan et al. have used new study to execution of VLSB-Steganography, where variable **numbers of *bits* for** gray scale image is used. The proposed study is called Varying-index-varying-bits-substitution (VIVBS). The aims of this paper is to overcome the drawback of DDDB and MDT methods in parameters of SNR- MSE and PSNR where these terms still not achieved as a perfect result. The proposed scheme is defines how much data which need to hidden in a pixel **with specific index** by calculated either x-intercept or y-intercept of pixel positions in cover image. The size of proposed key can be altered by changing a range of LSB utilized. In VIVBS algorithm, each pixel is processed and hiding a number of bits into pixel is depending to its index number [40].

Thakur et al. have carried out a novel security method based on image Steganography with cryptograph to hide secret image. The idea of the presented method is to encrypt the secret image using the proposed encryption scheme at first and then hides the encrypted image by Steganography scheme. The algorithm consists of two main sections. The first is to proposed encryption technique to encrypt the confidential image based on symmetric key concept. The second uses Steganography technique to hide the encrypted image using randomization techniques and LSB insertion [41].

Color image steganography system using hash function and edge detection technique in spatial domain has proposed by Singh et al. The canny edge has been applied on color image as a Edge detection scheme and then hash function HF algorithm is utilized to hide text message to the cover image (CI). The proposed scheme can be applied on many types of image formats like-jpg- jpeg, bmp-tiff etc [42].

Patel et al et al. have implemented and analyzed the steganography method and AES algorithm to make the evaluation and comparison into different formats of Images and gives the most suitable information with this technique. They are used LSB substitution algorithm in order to implementation Steganography method. This analysis and the evaluation is done with different parameters such as delay, PSNR, MSE, and Absolute Mean Square Error (RMSE) [43].

A new data hiding reversible technique using Pixel-Value-Difference (PVD) and Difference Expansion (DE) has introduced by Jana et al. The secret message is first divided into sub-stream of size n bits with proposed technique. Pixel Value Differencing (PVD) has been used to embed n−1 bits and 1 bit is ***embedded*** utilizing Difference-Expansion (DE). Finally, according to shared secret key bit stream, these the two-stego pixel pairs are distributing among dual image. The extract technique is the same embed technique in reverse sense [44].

Secure color image steganography through least significant bits (LSBs) has suggested by Al-Tamimi et al. Asymmetric key for image steganography is utilized in this scheme which is an array of 32 integers. Data hiding is inserted randomly according

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

to pixel selection generator and in hiding message; the transposition is applied to each 24-bit block. This helped to improved security on LSB substitution method [45].

A General Exploiting Modification Direction GEMD-map scheme has been proposed by Kuo et al. The objective of present work is increase capacity by reduced spatial redundancy in cover image. The cover image is partitioned into non-overlapping blocks based on scanning left to right and top to down pixels and partitions the secret message for each block using OGEs function [46].

A method for image steganography based on a combination of Cryptography and steganography has been described by Das. The objective of this research is using LSB substitution to hide multiple secret images in a single 24-bit. Before embedding, each message is encrypted utilizing Arnold-Transform (AT) algorithm. First three MSB-bits of the first *encrypted secret* image is concealment randomly in the last three LSB-bits of the red-pixels and then first three MSB bits of the second *and third encrypted* secret image SI is concealment randomly in the last three LSB-bits of the green *and blue pixels* respectively. The Stego-image SI is generated by combined the modified pixels [47].

Bhatt et al. Have used basic terminologies of image steganography and Visible Watermarking based on LSB Extraction Technique and Scale Invariant Feature Transform (SIFT). The ensures combination of both gives multiple layers of security and will achieve requirements like capacity, security and robustness [48].

A robust image steganography based on adaptive neural network with Genetic Algorithm has been proposed by El-Emama. The proposed system is more complexity to implementation due the deferent layers of security. The SPIHT algorithm has been applied to compress the secret message and then encrypted it using AES algorithm. Adaptive-image-segmentation (AIS) is utilized in this system as a new-adaptive-image-segmentation NAIS, this adaptive utilized to hide data randomly instead of sequentially [49]. Based on the review that has been carried out, it has been observed that researchers have proposed many techniques that have been used to enable the privacy of secret information when it is being transmitted. Such researchers have paid more attention to quality of image, payload, security and computational complexity. There is evidence that the extant techniques are accompanied by computational complexity. There are some of the methods that are some of the methods that are cost-effective and less computationally complex, but are unable to provide high quality of image, better security, and a higher payload. As a result of these limitations, they are undesirable alternatives when it comes to top-secret communication systems. In contrast, it has been observed that the method swhcih are complicated are able to offer higher payload, visual quality (VQ) and ***security***, but are expensive in terms of computation.

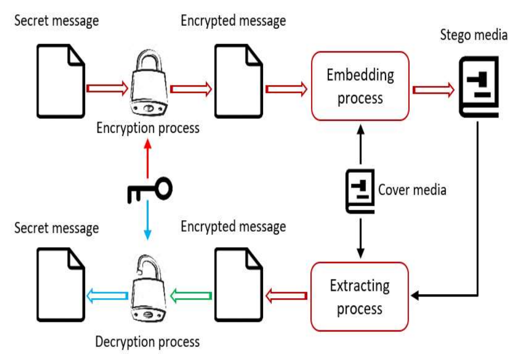

Figure 3. The combination of Steganography and cryptography.

2.1. Security Criteria

Security is salient topics in data-transmission and communication, especially in systems where security and privacy are requirements. Information hiding has two security. which consist steganography and encryption techniques, both of techniques play an important in term of data transmission security. Steganography strives to ensure secret messages are communicated securely by hiding them in carrier objects such as texts and pictures [50]. The structure of secret images secured through steganographic processes does not change, but concealed in the carrier media. so the security with steganography is represented with how to hide secret information by using high randomized algorithm. Several researchers are carried out to develop new randomize methods in steganography [51]. Majority of them considered random technique to enhance the privacy of the data due to its

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

simplicity and higher efficiency. Use of random generating algorithm consists many benefits such as:

- The security is more than others as it is like impossible or difficult to keep track of numbers in generating sequence by random process.
- The complexity is less & fast because of no need for rigid mathematical issue.
- More accurate and there is no duplication allowed for certain number in the sequence.

While cryptography alters the integrity of the transmitted information, such that it becomes meaningless to unauthorized persons except the communicating parties [52]. Steganography and cryptography have been noted to be individually insufficient for complete information security; therefore, a more reliable and strong mechanism can be achieved by combining both techniques. Combining these strategies can ensure an improved secret information security and will meet the requirements for security and robustness for transmitting important information over open channels. Figure 3 presents a strategy for the combination of both techniques.

3. PROPOSED SCHEME.

The suggested scheme and its main parts are discussed in detailed within this section. The pictorial details are aimed at presenting the novelty of the system to the readers with a clearer manner. The proposed scheme is developed for application on the colour image based on three parameters of henon map function for encryption and steganography.

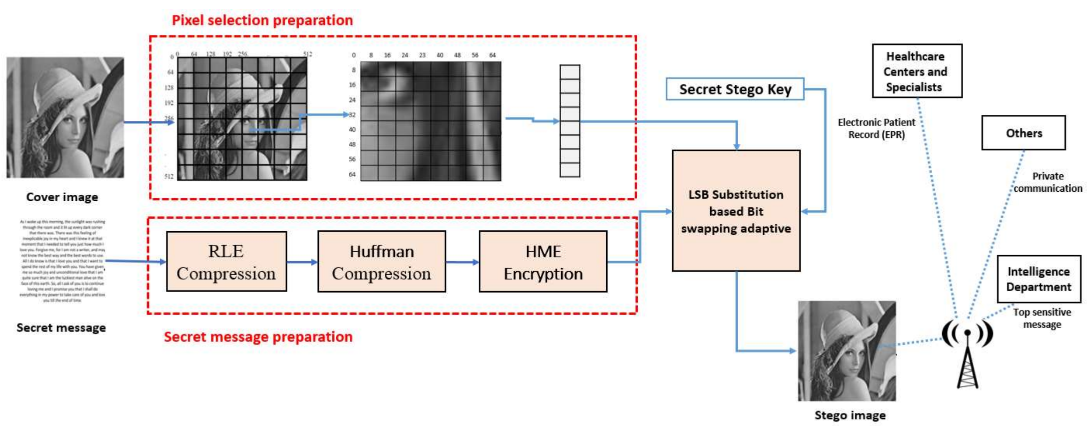

Figure 4. The entire diagram illustrating the proposed scheme

The proposed scheme (unlike the other steganography frameworks which have failed to achieve a suitable level of image quality and payload in a cost-effective way) can ensure a balance between payload, imperceptibility, computational complexity (CC) and robust (security) in a cost-effective way. The framework is ideal for application in the secure transmission of different secret bits, such as the *transmission* of Electronic-Patient-Records (EPR) to the health care centers, private communication which demands privacy, as well as sharing of top-secret sensitive communication between intelligence units. Figure 4 depicts a schematic representation of the suggested scheme in this study.

There are four main sub-algorithms in the proposed framework: 1) the HMC for the encryption of the secret text prior the embedding process (EP). The HMC was developed based the inspiration derived from [1] on the need to increase the security of secret information by introducing several barriers to invaders during the retrieval of secret information. Aziz et al. [53] suggested the use of the AES algorithm to encrypt secret information along with an encrypted secret key prior to the embedding process as used by [54]. Meanwhile, the AES algorithm was proven to be computationally costly and hence, cannot be applicable in real-time security applications [55, 56]. 2) Using two techniques RLE and Huffman to compress the secret text prior to embedding , this will also ensure an increase in the payload capacity. 3) Third algorithm is the text embedding framework which adaptively conceals the encrypted secret data in the carrier to produce the stego images that will be transmitted to the related units or users. 4) The final algorithm is the retrieval/extraction algorithm which retrieves the intended information from the stego image at the receivers' end for onward usage. Section 3 provides a brief overview of these algorithms.

3.1. Henon Map Cryptography (HMC)

To realize security criteria in proposed scheme, a new cryptography technique based on three parameters in order to enhance complicated. These parameters should test experimentally for adjustment then generated the key space that responsible for starting the encryption and keep tracking modification through our algorithm. The Henon map cryptography will used first to generate and match among generated vectors. Three vectors designed associated with three parameters generated sequentially one based on another's like loop of iterations. Dynamic key generating is very important and essential in text encryption then used in generating certain vector, generating number is limited (from 1to 26), according to alphabetic characters from A to Z.

For taken character from plain text, generated number will take effect on the next character associated with sequence in alphabetic order. New order selection algorithm suggested and encrypt becomes more complex and almost impossible indeed. Suggested algorithm include increasing the complexity of generating key space for number generator, this done by inserting second self-iteration for control parameters X. as shown in equation below:

(1)

Where n is starting the firs loop from 1 and ending with 26. X is considered the original sequence of the letter and Y is the character position in the cipher text. Security is an important due to the hacker and intruder always trying to find hidden message within image. Most of algorithms used by hacker check the sequence of normal random algorithm to find secret bits, and check familiar random sequence of embedding. For this reason new random sequence must be more complex.

Table 1. Illustration the Simple encryption of the word (COMPUTER)

C(1,3)	O(2,15)	M(3,13)	P(4,16)	U(5,21)	T(6,20)	E(7,5)	R(8,18)
I	K	N	V	H	A	L	W

In table 1 the coordinate of C(1,3) represent the first order in the text and the third order of letter C in alphabetic sequence. Second column represent the new generated order and corresponding order in alphabetic using the equation below:

$$Y_{new}=bX_{n-1} \text{ Mod } aX \quad (2)$$

All information will be saving in explicit key for using in the receiver side for decryption.

3.2 Hyper Compression

Second process for text before embedding stage will be the compression that reduces the text size using hyper compression first RLE then Huffman coding. The two algorithms can reduce the redundant text more as possible, the impact of using hyper compression that the Huffman some time fail to catch redundant letters if proceed 10 times for this reason can use RLE to support that. Because of sensitivity of the secret text, we use lossless encryption procedure to avoid missing the important information. The flowchart of each algorithm is shown in Figure 5.

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

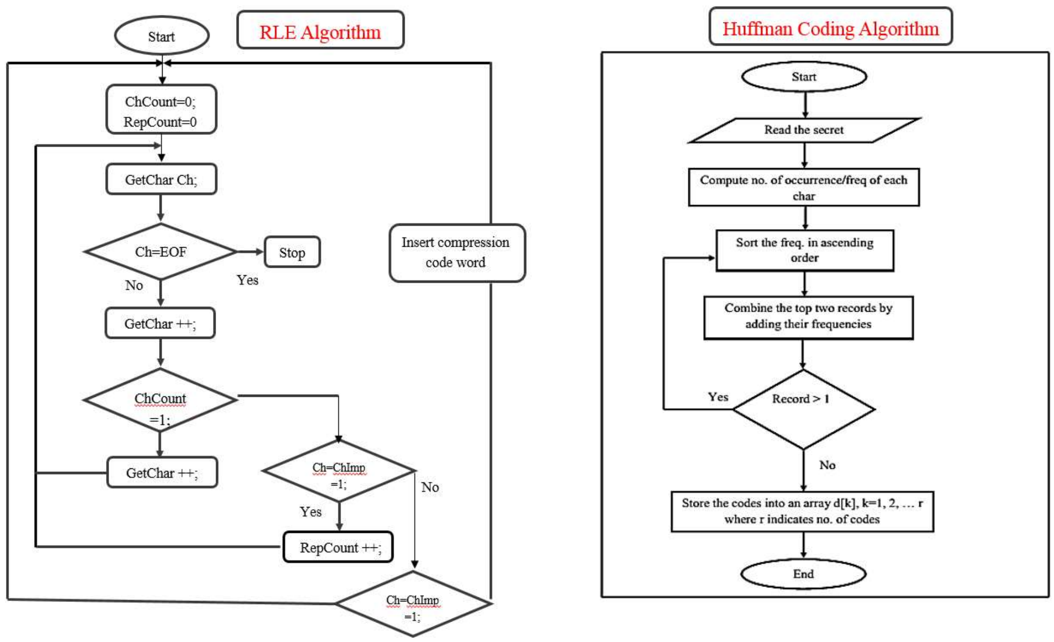

Figure 5. Flowchart of RLE and Huffman coding compression algorithms in proposed scheme.

Suggested technique for encryption can take the limit of generation key space and generation random number this number actually limit between 1 to 10 then assign another limit to the second vector between 1 to 100 and so on. Generating the number by proposed method has variable threshold or limit will chose experimentally then may change later for second iteration in the loop as shown in Figure 6.

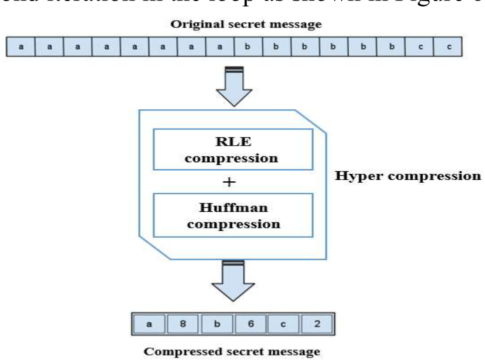

Figure 6. Illustrate the hyper compressions

Secret message will always be in the form of text, thus using hyper and Huffman is useful to compress this text message before proceeding with embedding process. Data preparation stage considers only the cover image and secret message process and the data is ready to be handled by other stages. This stage is considered the pre-processing stage. Good steganography technique has three aspects, maximum payload stored in the image, imperceptibility (visual quality VQ for image after embedding), and *robustness* so using hyper compression coding satisfies the first condition of the secret message capacity.

3.3 Embedding Stage

In our proposed method, two processes in side embedding stage (pixel selection strategy and embedding process) run simultaneously for inserting or hiding text message into an image. These two processes are briefly mention in the sub-sequent **sections**.

3.3.1 Pixel selection strategy

Most important aspect of embedding method is to find accurately that pixel, in which the secret message needs to be embedded. The problem is not just finding the location of embedment but the next location as well. In addition, the procedure to finding the full trajectory is also significant so that no one except the partner or receiver can track proposed algorithm. Selection of unpredictable paths for pixel is the main goal of each steganography designer. For these reasons, we involved Random technique with proposed system to increasing the probability of choosing the number up to , actually two control parameters used as a constant number in equation to increase the complexity of estimating numbers. Theoretical the two control parameters in random function give the possibility to discover the number by the hacker in one week with high performance computer. The cover image, firstly partitioned to 8×8 blocks each with 64×64 pixels. The process of selection will be occur randomly under Henon map function for blocks and then pixels, as shown in Figure 2. Henon map function is used to achieve objective of the security random function. These processes for selection blocks and pixels with proposed method illustrated in Figure 7.

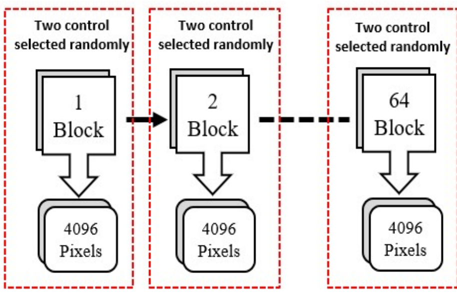

Figure 7. Illustrating the random selection pixels in proposed scheme.

Henon map function get 10^{30} attempt that gives around 2^{100} this is enough to secure the text inside the image. Normal random used single parameter to choose the number, initial condition for this function (single) is 10^{15} and probability of finding these numbers are 2^{50}. To increase the complexity of randomize the pixels selection, two control values are used to select the pixels for two stages (block and pixel selection). In steganography method the security play the important rule in order to avoid any hacker from discover our message in stego image, by this method finding secret message is almost impossible.

The Henon map function is an example of dynamic function system that behaviour been chaotic. Henon classical function have two control parameters a=1.4 and b=0.3 to be the chaotic. This function depends primary on a and b parameters, and to depict this function can illustrate as coordinate point (X_n, Y_n) in the plane. And new points conclude from this equation:

$$\begin{cases} x_{n+1} = 1 - a\,x_n^2 + y_n \\ y_{n+1} = b\,x_n \end{cases} \tag{3}$$

According to the statistics, an increase in the amount of data leads to less disturbance (messy) which means the stability of data distribution increased when increasing amount of data. We consider messy of reducing the data to embed the secret message through it, via making conditional map to embed the secret message. Generally three vectors (RND , PIX) are used to keep track of each pixel used with embedding process (for secret key) as shown in Figure 8.

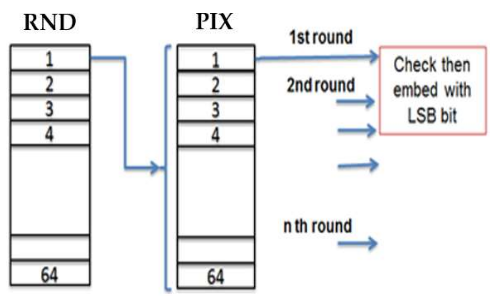

Figure 8. Main vectors used in Pixel selection strategy

First block comes from random stage consisting of 8 x 8 blocks (stored in RND vector) then continue with second random stage to select the destination pixel (stored in PIX vector).

3.3.2 Embedding algorithm EA

It is the responsibility of the embedding algorithm EA to hide the secret information within a cover image. The EA is able to conceal encrypted information within the LSB layer adaptively with the aid of the Stego-key SK. The major embedding mechanism steps of the proposed scheme is illustrated in algorithm 1. The most important procedure is to mark all the pixels into the block map called the Embedding block.

ALgorithm2: Embedding Algorithm

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

1. Initialize ← Cover Image , M ← Secret Message , ← Stego key
2. Apply RLE algorithm on M to get the compression bit stream ()
3. Apply Huffman coding algorithm on M^{CBS} to get the final compression bit stream
4. Apply HMC algorithm on to get encrypt secret information
5. Fragmentation the into groups each with 64 bits.
6. Select an appropriate cover image from dataset of cover images (
7. Divide I^C to three channels, resulting to R : red , G: green, B: Blue , channels as :- = (1, : ,:), = (:, 2 ,:), = (:, : , 3) , respectively.
8. Generate random number 1 and arrange it according to RND vector
9. Select one block of (8 x 8) blocks via RND vector
10. Generate random number 2 and arrange it according to PIX vector
11. Select destination pixel of (64 x 64) pixels via PIX vector
12. Mark the of each pixel and group
13 Generate M vector for embed process using and and Stego key
14 Let L <= length of
15 GLSB = get LSB (
16 If (GLSB ⊕
   a. Select channel
   b. Divide I^{CR} into two sections:
   c. $I^{CR} = LSB^{I^{CR}}(vector)$ and $MSB^{I^{CR}}(vector)$
   d. Replace $M^{ESI}(vector) \rightarrow LSB^{I^{CR}}(vector)$
   e. Rebuild pixel : $I^{CRS}(vector) = LSB^{I^{CR}}(vector) + MSB^{I^{CR}}(vector)$

Else
   a. Select I^{CB} channel
   b. Divide I^{CB} into two sections:
   c. $I^{CB} = LSB^{I^{CB}}(vector)$ and $MSB^{I^{CB}}(vector)$
   d. Replace $M^{ESI}(vector) \rightarrow LSB^{I^{CB}}(vector)$
   e. Rebuild pixel : $I^{CBS}(vector) = LSB^{I^{CB}}(vector) + MSB^{I^{CB}}(vector)$

END

17. I=I+1
18. Repeat Step 16 until all M^{ESI} are embedded, and the stego image is obtained.

Output: Stego Image (I^S)

For better understanding the mechanism of the EA, consider a color image *P* having pixels [P1, P2, P3, ... P8] in the binary form and encrypt the secret information (*Section 3.2*) M^{ESI} = (01110010)2. Here some of the intermediate steps are skipped in order to prevent confusion and misunderstanding of the central idea.

[P1: 11011110, 10000111, 11010110],
[P2: 11010101, 10010101, 10010110],
[P3: 11011010, 10110110, 11010111],
[P4: 11011010, 10110110, 11010111],
[P5: 10110110, 10100110, 11010111],
[P6: 11011110, 11010110, 11000110],
[P7: 11110110, 11010110, 11010110],
[P8: 11010111, 11100110, 11110110].

The beginning of the idea of the process of embedding started from pixel P1. Initially, the channel through which the secrete information *bit* will be concealed is determined using XOR bit operation of green channel LSB and encrypted secret information. The ***LSB*** of the green channel within pixel P1 is 1 *and the first bit* of M^{ESI} is 1. Result of XOR (1⊕0) = 1. Therefore, substitution of the LSB of blue channel of pixel P1 is made *with the first secret-bit* of M^{ESI}. The ***second*** pixel P2, (1⊕1) = 0,

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

substitute ***LSB*** of blue channel. For pixel P3, (0⊕1) = 1, substitute a ***LSB*** of red channel and *so on*. The pixels produced by the stego image are the pixels [P1 ′ , P2 ′ , P3 ′ ,... P8 ′].

[P1: 11011110, 10000111, 1101011**1**],
[P2: 1101010**0**, 10010101, 10010110],
[P3: 11011010, 10110110, 1101011**1**],
[P4: 11011010, 10110110, 1101011**1**],
[P5: 1011011**0**, 10100110, 11010111],
[P6: 11011110, 11010110, 1100011**0**],
[P7: 11110110, 11010110, 1101011**1**],
[P8: 11010111, 11100110, 1111011**0**].

Herein, the areas of embedment are reflected in the bold face LSBs in terms of pixels and channels. The changes made in the course of data hiding are reflected through the underlined LSBs on the bold face. Form the pixels of stego image, it can be clearly seen that about 40% of image pixels were modified. Furthermore, in the proposed approach an increase or decrease is made to the pixel value by just 1, and thus does not produce any detectable alteration of stego image.

3.4 Extracting algorithm

Extracting process aim to get the data from LSB pixels at the same time should follow the procedure designed and build in embedding process. Extracting process located in the other part (receiver) which includes procedure agreed by the two parties using stego key to guide the process. The procedure of extracting is like the embedding process but in reverse, that's mean that collect the components of the LSBs of the pixels and determine the pixel if it's 1 or 0. Most of variable information reflected by image and block partitioning, in additional to fragment of secret message. Such of this information called public information, while private information considered as the method followed by embedding process. The embedding and extracting processes are aimed at achieving two major objectives of security and imperceptibility as shown in figure 9.

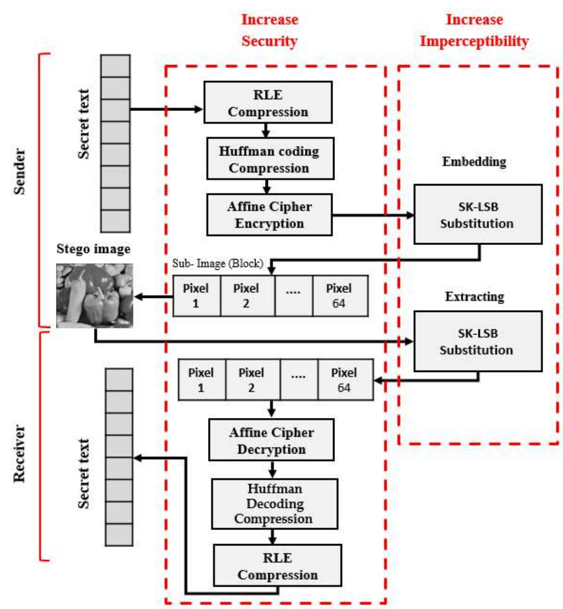

Figure 9. Two contributions within proposed scheme.

4. EXPERMANTAL RESULT

The setup for the experiment incudes eight standard colored images and MATLAB tool as presented in Figure 10. The eight images which possess a size of (512 x 512) are obtained from the *(USC-SIPI)* image database [57]. The *obtained* results are for the full capacity of each image for the different techniques methods. The respective stego-images (SI) for the proposed scheme (PS) for embedding percentage EP = 1 are presented in Figure 11. The techniques were experimentally evaluated based on parameters such as PSNR, EC, Structural Similarity Index (SSIM), and bits per pixel (BPP). The use of BER is employed in checking the robustness.

Journal of Theoretical and Applied Information Technology
15th August 2019. Vol.97. No 15

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

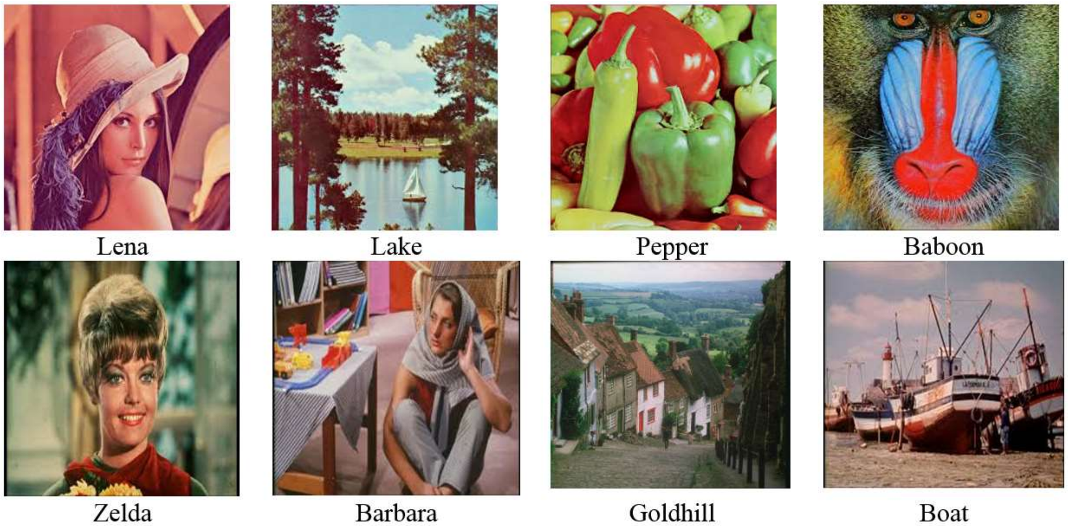

Figure 10 .Cover images used with proposed scheme.

4.1 Evaluation Based EC- PSNR- BPP and SSIM

The embedding capacity EC is defined as ratio between the number *of information bits* and number of carrier pixels [58, 2], which has directly relation with the number of pixels in our scheme because one pixels embeds different number of information bits.

$$C = \frac{The\ number\ of\ message\ bits}{The\ number\ of\ cover\ images's\ pixels} \quad (4)$$

Different payload capacity used with current study and reflected as a percentage to correspond with the researches in recent studies.

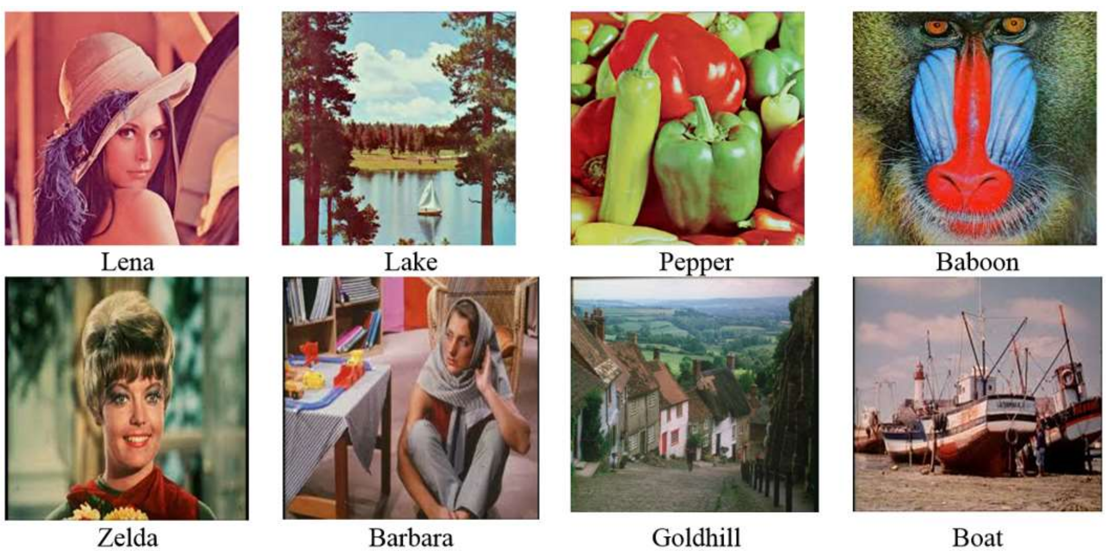

Figure 11 .Stego images for proposed scheme

Human Visual System (HVS) or Human Audio System (HAS) is an invisibility property, so no perceptible artifacts should be left if humans cannot differentiate carrier with or without hidden message [58]. 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 [32] .By applying the following equations PSNR can be calculated.

$$PSNR = 10log_{10}\left(\frac{255}{MSR}\right) \quad (5)$$

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

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij}) \quad (6)$$

Where, m and n are the images' sizes while x and y are the cover and stego images respectively. During the implementation of the proposed scheme two important stages were carried out on this study, namely the training and testing stages. In conventional processing of image, the imperceptibility of the stego image is measured using PSNR measures [59]. By applying the PSNR measures which mentioned above , the fidelity of the stego image is evaluated against the original carrier image. In other words, the level of distortion in the stego image is measured against the carrier image; this is measured in decibel (dB). If a higher score of PSNR is obtained, it means that the quality of the image is high, thereby minimizing the probability of detection using the HVS [70]. Through the training phase, PSNR is become less when the MSE is large, means mismatched increased between the original image and stego message. Whenever, MSE is large the result will be not good in term of PSNR because it works in a reverse as mention in equation (PSNR). This problem has been solved in testing stage and the result has been shown the better result from other methods. The BPP gives the average number of bits that can be hidden per pixel [59].

Table 2. Results for the proposed scheme and others methods with 12.5% EP

No	Image	PRT [65]	CRT [65]	Hashim [1]	Gui [66]	Muhammad [35]	Elshazly [68]	El-Emam [37]	Heidari [69]	Proposed scheme
1	Lena	52.38	52.91	66.40	35.39	51.13	55.48	53.60	55.34	66.61
2	Baboon	52.38	52.88	65.44	24.32	51.15	55.54	53.63	55.46	66.67
3	Pepper	52.39	52.89	66.45	35.38	51.14	55.18	52	55.35	66.60
4	Zelda	52.39	52.91	66.55	35.38	51.15	55.19	-	55.36	66.65
5	Barbara	52.39	52.89	-	33.49	51.10	55.19	53.60	55.32	66.60
	Average	**52.39**	**52.89**	**66.22**	**32.79**	**51.13**	**55.31**	**53.20**	**55.36**	**66.63**

In measuring the similarity between the original image and the stego-image, the use SSIM is utilized [59]. Eq. (7) is used in computing the similarity. The range of SSIM- value is from 1 to 1. If the SSIM-value is 1 that means , there is no difference between the original image (OI)and the stego-image (SI).

$$SSIM = \frac{(2P_O\, Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2\, Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2\,)} \quad (7)$$

For the original image, P_O, P_O^2 and σ_O^2 denote the mean *pixel value* , *variance and standard deviation* respectively. Likewise, for the stego-image, Q_S, Q_S^2 and σ_S^2 denote mean pixel value, *variance and* standard deviation respectively. rOS is the covariance between the original image (OI) and the stego-image (SI). The constant c1 = k1L and c2 = k2L, where k1 = 0.01, k2 = 0.03, and L is 255 for the grayscale image.

The proposed scheme results and the methods of Wu [60], Wn and Tsai's [61], Kumar and Chand's [62], Shahu [64] , Sahu & Swain's [63] and others, are presented in Tables 2, 3, 4, and 5. The PSNR of the proposed technique for embedding percentage EP= 6.25% is 72.74 dB and for EP = 12.5% it is 66.63 dB. The EC of the proposed technique is 131,072 and 265,144 bits for EP = 6.25% and 12.5% respectively.

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

Table 3. Results for the proposed scheme with 6.25% and 12.5% of EP.

Image (512 x 512)	Proposed Scheme (6.25%)				Proposed Scheme (12.5%)			
	PSNR	**EC**	**BPP**	**SSIM**	**PSNR**	**EC**	**BPP**	**SSIM**
Lena	72.58	131,072	0.5	1	66.61	265,144	1.0	0.99
Goldhill	72.58	131,072	0.5	1	66.62	265,144	1.0	0.99
Zelda	72.88	131,072	0.5	1	66.65	265,144	1.0	0.99
Pepper	72.63	131,072	0.5	1	66.60	265,144	1.0	0.99
Baboon	72.86	131,072	0.5	1	66.67	265,144	1.0	0.99
Boat	72.63	131,072	0.5	1	66.66	265,144	1.0	0.99
Lake	72.88	131,072	0.5	1	66.63	265,144	1.0	0.99
Barbara	72.90	131,072	0.5	1	66.61	265,144	1.0	0.99
Average	**72.74**	**131,072**	**0.5**	**1**	**66.63**	265,144	1.0	**0.99**

Table 4. The Wu [60] and Wu &Tsai's [61] techniques results

Image (512 x 512)	**Wu [60] (12.5%)**				**Wu &Tsai's [62]**			
	PSNR	***EC***	***BPP***	***SSIM***	***PSNR***	***EC***	***BPP***	***SSIM***
Lena	51.08	265,144	1.0	0.99	41.54	400,104	1.53	0.98
Goldhill	51.09	265,144	1.0	0.98	40.11	411,803	1.57	0.96
Zelda	51.09	265,144	1.0	0.98	40.01	399,029	1.52	0.97
Pepper	51.08	265,144	1.0	0.99	40.11	399,140	1.52	0.97
Baboon	51.07	265,144	1.0	0.98	39.03	419,209	1.6	0.97
Boat	51.08	265,144	1.0	0.98	39.23	411,764	1.57	0.97
Lake	51.07	265,144	1.0	0.98	39.47	401,249	1.53	0.97
Barbara	51.07	265,144	1.0	0.98	39.49	400,760	1.53	0.97
Average	**51.08**	**265,144**	**1.0**	**0.98**	**39.87**	**405,382**	**1.54**	**0.97**

In the studies carried out by Wu [60], and Kumar & Chand [62], PSNR of their techniques were 51.08 dB and 51.27 dB, respectively. As seen from the table of comparison, the proposed technique outperforms that of Wu [60] and Kumar & Chand [62] in terms of PSNR when EP= 12.5% with equal EC. The scores of the PSNR of the proposed scheme when EP= 6.25% and 12.5% is presented in Table 6. Based on the results, the marked images of the proposed scheme are of better quality, thereby confirming its effectiveness. The PNSR obtained in the techniques proposed by Wn technique [60], Wu and Tsai technique [61] and Kumar & Chand [62] is good, however, Wu and Tsai technique [61] obtained a low EC. Table 6. shows the average time used in embedding data, as well as the average PSNR on USC-SIPI. Variations in the average embedding time was observed, varying from 0.1 seconds to 0.12 seconds for different payloads. The proposed scheme modifies maximum of two least significant bits, and so the quality of image does not deteriorate. Variations in the calculated average PSNR was observed within the range of 72.82 at 6.25% of EP to 66.64 at 12.5% of EP.

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

Table 5. The Kumar & Chand's [62] and Sahu [64] techniques Results

Image (512 x 512)	Kumar & Chand's (12.5%) [62]				Sahu (18.75%) [64]			
	PSNR	EC	BPP	SSIM	PSNR	EC	BPP	SSIM
Lena	51.27	265,144	1.0	0.98	47.38	393,216	1.5	0.97
Pepper	51.28	265,144	1.0	0.98	47.39	393,216	1.5	0.97
Baboon	51.27	265,144	1.0	0.99	47.36	393,216	1.5	0.99
Boat	51.27	265,144	1.0	0.99	47.20	393,216	1.5	0.98
Barbara	51.28	265,144	1.0	0.99	47.37	393,216	1.5	0.98
Average	**51.27**	**265,144**	**1.0**	**0.99**	**47.34**	**393,216**	**1.5**	**0.98**

Table 6. Average execution time and PSNR on USC-SIPI images

Embedding payload (%)	Bit per pixel (BPP)	Average time (Second)	Average PSNR
6.24 %	0.5	0.1010	72.74
12.5 %	1.0	0.1235	66.63

4.2 Robustness Evaluation for the proposed scheme Against Bit Error Rate (BER)

The robustness of the proposed scheme was evaluated using two traditional quantities, which is bit error rate (BER). Robustness refers to the ability of the secret bits to resist attacks, which are referred to as hereunder.

Table 7. Bit Error Rate (BER) for the proposed scheme in our simulations when EP= 6.25%, 12.5%

Image (512 x 512)	Proposed Scheme (6.25%)				Proposed Scheme (12.5%)			
	PSNR	EP	BER	BER-P	PSNR	EP	BER	BER-P
Lena	72.58	6.25%	0.01377	1.37%	66.61	12.5%	0.01501	1.50%
Goldhill	72.58	6.25%	0.01377	1.37%	66.62	12.5%	0.01501	1.50%
Zelda	72.88	6.25%	0.01372	1.37%	66.65	12.5%	0.01500	1.50%
Pepper	72.63	6.25%	0.01376	1.37%	66.60	12.5%	0.01501	1.50%
Baboon	72.86	6.25%	0.01372	1.37%	66.67	12.5%	0.01499	1.49%
Boat	72.63	6.25%	0.01376	1.37%	66.66	12.5%	0.01500	1.50%
Lake	72.88	6.25%	0.01372	1.37%	66.63	12.5%	0.01501	1.50%
Barbara	72.90	6.25%	0.01371	1.37%	66.61	12.5%	0.01501	1.50%
Average	**72.74**	**6.25%**	**0.01373**	**1.37%**	**66.63**	**12.5%**	**0.01500**	**1.50%**

The value of PSNR is inverted so as to obtain the bit error rate using the following equation:

$$BER = 1/PSNR \quad (8)$$

The portion of the original image's (OI) 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 6 present the results of the calculated BER in the simulation of the current study, while Tables 7, 8 and 9 present the results obtained for other techniques proposed in previous studies.

Journal of Theoretical and Applied Information Technology
15th August 2019. Vol.97. No 15

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

Table 8. Bit Error Rate (BER) for the Wu [60] and Wu &Tsai's [61] techniques.

Image (512 x 512)	Wu [60] (12.5%)				Wu &Tsai's [61]			
	PSNR	EP	BER	BER-P	PSNR	EP	BER	BER-P
Lena	51.08	12.5%	0.01957	1.95%	41.54	N/A	0.02407	2.40%
Lighthouse	51.09	12.5%	0.01957	1.95%	40.11	N/A	0.02493	2.49%
Zelda	51.09	12.5%	0.01957	1.95%	40.01	N/A	0.02499	2.49%
Pepper	51.08	12.5%	0.01957	1.95%	40.11	N/A	0.02493	2.49%
Baboon	51.07	12.5%	0.01958	1.95%	39.03	N/A	0.02562	2.56%
Boat	51.08	12.5%	0.01957	1.95%	39.23	N/A	0.02549	2.54%
House	51.07	12.5%	0.01958	1.95%	39.47	N/A	0.02533	2.53%
Couple	51.07	12.5%	0.01958	1.95%	39.49	N/A	0.02532	2.53%
Average	**51.08**	**12.5%**	**0.01957**	**1.95%**	**39.87**	N/A	**0.02513**	**2.51%**

Table 9. Bit Error Rate (BER) for the Kumar & Chand's [62] and Sahu [64] techniques.

Image (512 x 512)	Kumar & Chand's [62] (12.5%)				Sahu's (18.75%) [64]			
	PSNR	EP	BER	BER-P	PSNR	EP	BER	BER-P
Lena	51.27	12.5%	0.01950	1.95%	47.38	18.75%	0.02110	2.11%
Pepper	51.28	12.5%	0.01950	1.95%	47.39	18.75%	0.02110	2.11%
Baboon	51.27	12.5%	0.01950	1.95%	47.36	18.75%	0.02111	2.11%
Boat	51.27	12.5%	0.01950	1.95%	47.20	18.75%	0.02118	2.11%
House	51.28	12.5%	0.01950	1.95%	47.37	18.75%	0.02110	2.11%
Average	**51.27**	**12.5%**	**0.01950**	**1.95%**	**47.34**	**18.75%**	**0.02112**	**2.11%**

The BER and BER-P of the proposed scheme for embedding percentage EP= 6.25% is 0.01373 and 1.37% and for EP = 12.5% it is 0.01500. The BER and BER-P of the techniques proposed by Wu [60] and Kumar & Chand technique [62] are 0.01957, 1.95% and 0.01950, 1.95% respectively. Based on the results of the current study, the proposed scheme produced better BER and BER-P than that of Wu [60] and Kumar & Chand [62] when EP= 12.5% with equal EC.

From the above empirical results, we can see the distortion rate (imperceptibility) of image and hiding capacity comparison with others. Therefore, the proposed method is reduced the distortion on the cover image with high hiding capacity. We have considers some disadvantage (weakness) and tried to overcome some problem and still some improvement needed with future work.

Based on the results obtained for the experiments for the proposed scheme, it is concluded that the proposed scheme can be used with different kinds of medical images like MRI and CTScan images. More so, the proposed method is capable of providing different potential applications in the field of medicine. With this, patients in remote areas can be medically diagnosed through remote monitoring centers.

However, proposed method has limitations in term of capacity, so increase the capacity will degradation image quality (imperceptibility) and other limitation in proposed method, four dataset only have been tested within this method.

5. Conclusion

Several digital image steganography methods has been introduced, all are focused based payload and image quality. Moreover, there is a trade-off amidst

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

these two metrics and saving a better balance amidst them is yet a challenging case. Therefore, previous methods fail to realize a high security level because to direct embedding secret information inside image without cryptography consideration, making information extraction relatively simple for adversaries. So, the new secure steganography scheme has been proposed to combines the benefits of cryptography method and steganography with the aim of achieving the better security using new encryption method based on three parameters, and to reduce the modification per pixel value which indirectly increases the visual quality of stego-image by using a new hiding scheme. The objectives of paper to increase the security and PSNR of the stego image . The Hyper technique has been used to compress the secret information prior to embedding, this will also ensure an increase in the payload capacity. The proposed scheme takes effect after compressing and encrypting the secret information. This algorithm is provide differnt security layers worked together to augment protection of attacks. The experimental results shows the efficient scheme from PSNR , SSIM and payload for evaluating the stego image compared to the existing methods.

REFERENCE

[1] 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, no. 22 (2017).

[2] Rabie T, Baziyad M, Bonny T ,"Toward a unified performance measure for steganography systems" . Multimed Tools Appl, submitted. (2018)

[3] 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.

[4] Sharma, Vijay Kumar, Pratistha Mathur, and Devesh Kumar Srivastava. "Highly Secure DWT Steganography Scheme for Encrypted Data Hiding." In Information and Communication Technology for Intelligent Systems, pp. 665-673. Springer, Singapore, 2019.

[5] Tang, Mingwei, Shenke Zeng, Xiaoliang Chen, Jie Hu, and Yajun Du. "An adaptive image steganography using AMBTC compression and interpolation technique." Optik-International Journal for Light and Electron Optics 127, no. 1 (2016): 471-477.

[6] HASHIM, MOHAMMED, MOHD RAHIM, MOHD SHAFRY, and ALI ABDULRAHEEM ALWAN. "A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN." Journal of Theoretical & Applied Information Technology 96, no. 4 (2018).

[7] Anderson, Ross J., and Fabien AP Petitcolas. "On the limits of steganography." IEEE Journal on selected areas in communications 16, no. 4 (1998): 474-481.

[8] Chen, Brian, and Gregory W. Wornell. "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding." IEEE Transactions on Information Theory 47, no. 4 (2001): 1423-1443.

[9] Kaw, Javaid A., Nazir A. Loan, Shabir A. Parah, K. Muhammad, Javaid A. Sheikh, and G. M. Bhat. "A reversible and secure patient information hiding system for IoT driven e-health." International Journal of Information Management 45 (2019): 262-275.

[10] Bhattacharyya, Souvik, and Gautam Sanyal. "A robust image steganography using DWT difference modulation (DWTDM)." International Journal of Computer Network and Information Security 4, no. 7 (2012): 27.

[11] Qin, Chuan, Chin-Chen Chang, and Chia-Chun Lin. "An adaptive reversible steganographic scheme based on the just noticeable distortion." Multimedia Tools and Applications 74, no. 6 (2015): 1983-1995.

[12] Mielikainen, Jarno. "LSB matching revisited." IEEE signal processing letters 13, no. 5 (2006): 285-287.

[13] Muhammad, Khan, Muhammad Sajjad, and Sung Wook Baik. "Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy." Journal of medical systems 40, no. 5 (2016): 114.

[14] Qazanfari, Kazem, and Reza Safabakhsh. "A new steganography method which preserves

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

histogram: Generalization of LSB++." Information Sciences 277 (2014): 90-101.

[15] Prasad, Shiv, and Arup Kumar Pal. "Logistic Map-Based Image Steganography Scheme Using Combined LSB and PVD for Security Enhancement." In Emerging Technologies in Data Mining and Information Security, pp. 203-214. Springer, Singapore, 2019.

[16] Ansari, Ebrahim, Morteza Keshtkaran, Richard Wallace, S. M. H. Mirsadeghi, and Fateme Ansari. "OOPAP and OPVD: Two Innovative Improvements for Hiding Secret Data Into Images." Iranian Journal of Science and Technology, Transactions of Electrical Engineering 43, no. 1 (2019): 55-65.

[17] Hu, WenWen, Ri-Gui Zhou, Jia Luo, and BiYing Liu. "LSBs-based quantum color images watermarking algorithm in edge region." Quantum Information Processing 18, no. 1 (2019): 16.

[18] Banik, Barnali Gupta, Manish Kumar Poddar, and Samir Kumar Bandyopadhyay. "Image Steganography Using Edge Detection by Kirsch Operator and Flexible Replacement Technique." In Emerging Technologies in Data Mining and Information Security, pp. 175-187. Springer, Singapore, 2019.

[19] Mukherjee, Srilekha, and Goutam Sanyal. "Edge based image steganography with variable threshold." Multimedia Tools and Applications (2018): 1-26.

[20] Joshi, Kamaldeep, Swati Gill, and Rajkumar Yadav. "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image." Journal of Computer Networks and Communications 2018 (2018).

[21] Long, Min, and Fenfang Li. "A Formula Adaptive Pixel Pair Matching Steganography Algorithm." Advances in Multimedia 2018 (2018).

[22] Rabie, Tamer, Mohammed Baziyad, and Ibrahim Kamel. "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid." Multimedia Tools and Applications 77, no. 18 (2018): 23673-23698.

[23] Evsutin, Oleg, Anna Kokurina, Roman Meshcheryakov, and Olga Shumskaya. "The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation." Multimedia Tools and Applications 77, no. 21 (2018): 28567-28599.

[24] 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 (2018): 1-19.

[25] Patidar, Rohit, Balwant Prajapat, and Anwar Sakreja. "Image Steganography Based on Random Pixel Addition and Discrete Cosine Transform (DCT)." In International Conference on Advanced Computing Networking and Informatics, pp. 453-458. Springer, Singapore, 2019.

[26] Li, Jianzhong, Chuying Yu, B. B. Gupta, and Xuechang Ren. "Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition." Multimedia Tools and Applications 77, no. 4 (2018): 4545-4561.

[27] 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.

[28] 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.

[29] DOMAIN, WATERMARKING TECHNIQUES IN SPATIAL. "A REVIEW AND OPEN ISSUES OF DIVERSE TEXT WATERMARKING TECHNIQUES IN SPATIAL DOMAIN." Journal of Theoretical and Applied Information Technology 96, no. 17 (2018).

[30] Dhargupta, S., A. Chakraborty, S. K. Ghosal, S. Saha, and R. Sarkar. "Fuzzy edge detection based steganography using modified Gaussian distribution." Multimedia Tools and Applications (2019): 1-18.

[31] Ali, Ahmed Hussain, Mohd Rosmadi Mokhtar, and Loay Edwar George. "ENHANCING THE HIDING CAPACITY OF AUDIO STEGANOGRAPHY BASED ON BLOCK MAPPING." Journal of Theoretical & Applied Information Technology 95, no. 7 (2017).

[32] Wu, Ben, Matthew P. Chang, Bhavin J. Shastri, Phillip Y. Ma, and Paul R. Prucnal. "Dispersion deployment and compensation for optical steganography based on noise." IEEE Photonics Technology Letters 28, no. 4 (2016): 421-424.

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

[33] Sedighi, Vahid, Rémi Cogranne, and Jessica Fridrich. "Content-adaptive steganography by minimizing statistical detectability." IEEE Transactions on Information Forensics and Security 11, no. 2 (2016): 221-234.
[34] Seyyedi, Seyyed Amin, Vasili Sadau, and Nick Ivanov. "A Secure Steganography Method Based on Integer Lifting Wavelet Transform." IJ Network Security 18, no. 1 (2016): 124-132.
[35] Muhammad, Khan, Jamil Ahmad, Naeem Ur Rehman, Zahoor Jan, and Muhammad Sajjad. "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method." Multimedia Tools and Applications 76, no. 6 (2017): 8597-8626.
[36] Jiang, Nan, Na Zhao, and Luo Wang. "LSB based quantum image steganography algorithm." International Journal of Theoretical Physics 55, no. 1 (2016): 107-123.
[37] El-Emam, Nameer N., and Mofleh Al-Diabat. "A novel algorithm for colour image steganography using a new intelligent technique based on three phases." Applied Soft Computing 37 (2015): 830-846.
[38] Sun, Shuliang. "A novel edge based image steganography with 2k correction and Huffman encoding." Information Processing Letters 116, no. 2 (2016): 93-99.
[39] 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.
[40] 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.
[41] Thakur, Priyanka, Santosh Kushwaha, and Yogesh Rai. "Enhance Steganography Techniques: A Solution for Image Security." International Journal of Computer Applications 115.3 (2015).
[42] Singh, Saurabh, and Ashutosh Datar. "Improved hash based approach for secure color image steganography using canny edge detection method." International Journal of Computer Science and Network Security (IJCSNS) 15.7 (2015): 92.
[43] Patel, Farah R., and A. N. Cheeran. "Performance Evaluation of Steganography and AES encryption based on different formats of the Image." Performance Evaluation 4.5 (2015).
[44] 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.
[45] 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.
[46] Kuo, Wen-Chung, et al. "Secure multi-group data hiding based on gemd map." Multimedia Tools and Applications 76.2 (2017): 1901-1919.
[47] Das, Pallavi, Satish Chandra Kushwaha, and Madhuparna Chakraborty. "Multiple embedding secret key image steganography using LSB substitution and Arnold transform." Electronics and Communication Systems (ICECS), 2015 2nd International Conference on. IEEE, 2015.
[48] Bhatt, Santhoshi, et al. "Image steganography and visible watermarking using LSB extraction technique." Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on. IEEE, 2015.
[49] Pradhan, Anita, Aditya Kumar Sahu, Gandharba Swain, and K. Raja Sekhar. "Performance evaluation parameters of image steganography techniques." In 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), pp. 1-8. IEEE, 2016.
[50] Feng, Bingwen, Wei Lu, and Wei Sun. "Secure binary image steganography based on minimizing the distortion on the texture." IEEE transactions on Information Forensics and Security 10, no. 2 (2015): 243-255.
[51] Bucerzan, Dominic, and Crina Raţiu. "Image processing with android steganography." In International Workshop Soft Computing Applications, pp. 27-36. Springer, Cham, 2014.
[52] Muhammad, Khan, Jamil Ahmad, Haleem Farman, Zahoor Jan, Muhammad Sajjad, and Sung Wook Baik. "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption." TIIS 9, no. 5 (2015): 1938-1962.

[53] Aziz, Mahdi, Mohammad H. Tayarani-N, and Mehdi Afsar. "A cycling chaos-based cryptic-free algorithm for image steganography." Nonlinear Dynamics 80, no. 3 (2015): 1271-1290.
[54] Nguyen, Tuan Duc, Somjit Arch-Int, and Ngamnij Arch-Int. "An adaptive multi bit-plane image steganography using block data-hiding." Multimedia Tools and Applications 75, no. 14 (2016): 8319-8345.
[55] Jingmei, Liu, Wei Baodian, and Wang Xinmei. "One AES S-box to increase complexity and its cryptanalysis." Journal of Systems Engineering and Electronics 18, no. 2 (2007): 427-433.
[56] Liu, Quan, Pei-yue Li, Ming-chao Zhang, Yong-xin Sui, and Huai-jiang Yang. "A novel image encryption algorithm based on chaos maps with Markov properties." Communications in Nonlinear Science and Numerical Simulation 20, no. 2 (2015): 506-515.
[57] USC-SIPI Image Database (Online). Available http://sipi.usc.edu/database/database.php?volume=misc. Accessed 14 June 2018.
[58] Chen, Wen-Yuan. "Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques." Applied Mathematics and computation 196, no. 1 (2008): 40-54.
[59] Hashim, Mohammed Mahdi, Mohd Shafry Mohd Rahim, Fadil Abass Johi, Mustafa Sabah Taha, and Hassan Salman Hamad. "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats." International Journal of Engineering & Technology 7, no. 4 (2018): 3505-3514.
[60] Wu, Nan-I., and Min-Shiang Hwang. "A novel LSB data hiding scheme with the lowest distortion." The Imaging Science Journal 65, no. 6 (2017): 371-378.
[61] Wu, Da-Chun, and Wen-Hsiang Tsai. "A steganographic method for images by pixel-value differencing." Pattern Recognition Letters 24, no. 9-10 (2003): 1613-1626.
[62] Kumar, Rajeev, and Satish Chand. "A reversible data hiding scheme using bit flipping strategy." Journal of Discrete Mathematical Sciences and Cryptography 19, no. 2 (2016): 331-345.
[63] Sahu, Aditya Kumar, and Gandharba Swain. "A Novel n-Rightmost Bit Replacement Image Steganography Technique." 3D Research 10, no. 1 (2019): 2.
[64] 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.
[65] 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 (2018): 1-18.
[66] Sheth, Utsav, and Shiva Saxena. "Image steganography using AES encryption and least significant nibble." In 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 0876-0879. IEEE, 2016.
[67] Muhammad, Khan, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik. "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks." Future Generation Computer Systems 86 (2018): 951-960.
[68] Elshazly, E. A., Safey AS Abdelwahab, R. M. Fikry, S. M. Elaraby, O. Zahran, and M. El-Kordy. "FPGA implementation of robust image steganography technique based on least significant bit (LSB) in spatial domain." International Journal of Computer Applications 145, no. 12 (2016): 43-52.
[69] Heidari, Shahrokh, Mohammad Rasoul Pourarian, Reza Gheibi, Mosayeb Naseri, and Monireh Houshmand. "Quantum red–green–blue image steganography." International Journal of Quantum Information 15, no. 05 (2017): 1750039.
[70] Hashim, Mohammed Mahdi, Mohd Shafry Mohd Rahim, Fadil Abass Johi, Mustafa Sabah Taha, Ali A. Al-Wan, and Nilam Nur Amir Sjarif. "An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching." International Journal of Engineering & Technology 7, no. 4 (2018): 4008-4023.
[71] Mahdi, Mohammed Hashim, Ali Abdulwahhab Abdulrazzaq, Mohd Shafry Mohd Rahim, Mustafa Sabah Taha, Hiyam Nadhim Khalid, and Sameer Abdulsattar Lafta. "Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption." In *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, p. 052002. IOP Publishing, 2019.

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

[72] Taha, Mustafa Sabah, Mohd Shafry Mohd Rahim, Sameer Abdulsattar Lafta, Mohammed Mahdi Hashim, and Hassanain Mahdi Alzuabidi. "Combination of Steganography and Cryptography: A short Survey." In *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, p. 052003. IOP Publishing, 2019.