Secure Image Steganography Through Multilevel Security

Ali Salem Ali[a], Mohammed Sabbih Hamoud Al-Tamimi[b], Alaa Ahmed Abbood[c], [a]Department of Network Engineering , Al-Iraqia University ,Adamyia, Baghdad,Iraq, [b]Department of Computer Science, College of Science, University of Baghdad, [c]University of information technology and communications, Email: [a]Alialbander2004@yahoo.com, [b]m_altamimi75@yahoo.com, [c]aaalaa2@uoitc.edu.iq

The concealment of data has emerged as an area of deep and wide interest in research that endeavours to conceal data in a covert and stealth manner, to avoid detection through the embedment of the secret data into cover images that appear inconspicuous. These cover images may be in the format of images or videos used for concealment of the messages, yet still retaining the quality visually. Over the past ten years, there have been numerous researches on varying steganographic methods related to images, that emphasised on payload and the quality of the image. Nevertheless, a compromise exists between the two indicators and to mediate a more favourable reconciliation for this duo is a daunting and problematic task. Additionally, the current techniques have not been successful in attaining more improved security caused by the non-encrypted data that only underwent the first layer of concealment through merely a straightforward embedment process of the secret data within the images, thus allowing the extraction of the concealed data to be quite simple for hostile entities. Hence, in the current study, the proposed scheme, we have improved the Bit Inverting Map method to narrow the gap of existing work. Our experimental results indicate that the proposed framework maintains a better balance between image visual quality and security, with relatively less computational and complexity, which assures its effectiveness compared to other state-of-the-art methods.

Key words: *Security system, Steganography, Image carries, Stego-image, BIM.*

Introduction

The heightened relaying of secret data through unsecure internet channels has resulted in a problematic situation of protecting sensitive data, and this concern has become an emerging area of great interest in the scientific domain encompassing the past decades. The procedure discovered that have been able to resolve the issue on data security in a favourably for quite some time now is Cryptography. This technique involves the scrambling of the sensitive data by making it appear senseless through the process of data encryption (Sabah, et al.,2019). Nevertheless, the core challenge in techniques using cryptography is the glaring, conspicuous meaningless manner of the encrypted data, causing them to be undue attention grabbers as to arouse suspicions in the hostile entities. As a result, this will lead to the use of forceful cryptanalysis systems for the decryption of the encrypted data by hostile entities (Nicolas, et al.,2019). However, the resolution to this issue is through the implementation of data concealment techniques like "steganography", to conserve the sensitive data at the time of data relaying, and at the same time, ensuring a high level of security (Hashim, et al.,2019).

The etymology of Steganography comes from a Greek source that signified covered writing. Specifically designed for the concealment of data, it is regarded as the scientific method for undetected communications, with the main objective of an unnoticeable concealment ofsecret data within a cover object such as image, where the presence of the secret data is a shared knowledge only between the transmitter and recipient (Mahdi, et al.,2018). The steganographic components are the sensitive data, the cover object, a method for the embedment, and a stego key for heightened security. The cover object can be in the form of text, internet protocol, image, DNA and video. The application for Steganography extensive, like in the wireless sensor body area network used for healthcare (Sabah, et al.,2018), security in voting systems, enhancing security in mobile banking, telemedicine in wellbeing sectors, and secret transactions between two entities (Mahdi, et al.,2018; Sabah, et al.,2018). It has abundant usage; nonetheless, there are also risks involved because hackers also utilise it to transmit Trojans and viruses that will magnify the compromise of sensitive systems. Furthermore, it may be utilised in terrorism and crime acts in the exchanges of secret data (Choudhary,2012). Varying methods are utilised in image steganography. The initial image is the cover image that contains no concealed secret data; with an outcome image known as the stego image after the embedment of the secret data into the cover image, and the stego key is also known as the secret key is used during the embedment procedure, which enhanced the security.

The secret data may be in the form of a text data, in sound form, in video form or an image form. The embedment capacity is termed as the ‘Payload’, and entails the number of secret data which is concealable within a cover image free of visual artifacts within stego images. The measurement of the payload capacity is gauged as in bits per pixel (bpp). Hence, in instances when a one-bit data is concealed in each pixel, the steganographic algorithm payload is 1bpp. The payload magnitude is proportional to the powerfulness of the steganographic algorithm or otherwise (Wang, and Ishbel,2019). The steganographic robustness entails the steganographic algorithm consistency in countering various kinds of statistical attacks. The intensity of the steganographic algorithm robustness is gauged from the ability to embed the data within the cover image without allowing its easy extraction or modifications by the image processing activities, such as image noising, scaling, rotation and cropping. However, the issue of robustness is often considered in watermarking methods as a result of concerns pertaining to copyright protection (Yi, et al.,2019).

Imperceptibility is another term another core concern in steganography as it entails the inconspicuousness of data and gauges in numerous different image quality in terms of as peak-signal-to-noise-ratio (PSNR), root-mean-square-error (RMSE), and structural-similarity-indexmetric (SSIM). A steganographic technique is considered to be extremely imperceptible on the condition that it generates stego images that possess the minimal probable deformation following the deliberate concealment of the data, and that it is difficult to discover the through the human visual system (HVS) (Wang, and Ishbel,2019). Saw that the process of data embedment in image steganography methods are categorised into the spatial domain which is an Image domain, and transform domain which is a frequency domain. The spatial domain method is according to a straightforward adjustment of pixel intensities, possessing a bigger embedding capability with a moderate deterioration on the quality of the image. The aforementioned techniques have lower robustness due to the embedment of data procedure that may not be completely retrieved. In instances when the stego images are visible for the manipulation of the image and are susceptible to attacks such as cropping, noise being added to it, being compressed, being filtered, being rotated, and being translated, of which these are its restrictions. Certain spatial domain techniques consist of the Least Significant Bit substitution techniques (Sajjad, and Sung,2016), tri-way-pixel-value-differencing method (Yen-Po, et al.,2011), grey-level modification methods (Sabah, et al.,2019; Kumar, and Gandharba,2019), edges-based embedding methods (Islam, and Phalguni,2013), pixel indicator techniques (PIT) (Kingsly Infant, and J. B,2014), and pixel-pair-matching method (Chen,2014). The Transform domain methods are founded on the use of transformed coefficients for the embedding of data, possessing minimal susceptibility to various attacks. Certain popular methods in this classification are the Discrete Cosine Transform technique, Discrete Wavelength Transform technique, Discrete Fourier Transform technique, and Integer Contour Transform technique (Kamel, and Mohammed,2018).

The Transform domain technique possesses greater robustness in comparison to the spatial domain technique, thus enabling them greater aptness to be used for watermarking objectives like copyright protection (Baziyad, and Ibrahim,2018). The biggest disadvantage of the techniques as mentioned above is that they possess inferior payload and large computations that are complicated, and result infailure in maintaining a superior equilibrium between the quality of the image, security, effectiveness, and the payload capacity, thus causing them to be an unfavourable choice for real-time security usage. Taking into consideration the mentioned restrictions, our technique which was founded on the spatial domain, that was created.

Traversing the last decades, there were numerous development of spatial domain steganographic techniques which were introduced. The Least Significant Bit (LSB) substitution technique the most popular technique that involves the LSBs of the cover image to be substituted with data, resulting in relatively favourable marked images quality. Nevertheless, its simplicity and disparate pixels modification has resulted in it being more conspicuous and easily detected by the steganalysis system (Pallavi, and Vijay,2019). The said constraint is kept to a minimal by the LSB-matching (LSBM) scheme (Huang, and Jiwu,2010). through the addition/subtraction of a numerical one to the pixels in the cover image according to the secret data, decreasing the probability of being detected, however having certain deformity on the marked images. The LSBM revisited (LSBMR) (Zhang, and Baoji,2013).enhances the LSBM scheme through factoring in the association between a couple of pixel duos for the concealment of two bits at one time, decreasing the degree of deformation for marked images to the limits of 0.325 from 0.5 bpp. According to the work of (Luo et al.,2010), they lowered the perceptibility through the combination of the LSBMR with concealment mechanism that is edge-based, choosing via adaptive methods the cover image areas for the hiding of data according to the needs. The aforementioned schemes under review are vulnerable to various challenges like:

i) The straightforward embedment of sensitive data within the cover image by not taking into account encryption, that allows attackers to be able to engage in the extraction of the secret data with not much difficulty when the algorithm used for embedment is deciphered ii) the formation of deformed stego image that can be discerned visually is produced due to the ineffective embedding algorithms used, that had increased the probability of perceptibility by the HVS, and iii) the absence of sustaining a suitable equilibrium between the quality of the image, the payload, the complicatedness of the computation, and the security, that causes a reduction in its appropriateness for real-time and confidential security implementations.
Through our current research, the said challenges are looked into through our recommendation of using an effective technique for grey and colour images within the spatial domain, by using adaptive LSB replacement method with Advanced Encryption Standard (DES) cryptography. Our fundamental research offering of are outlined in brief as the following:

The rest of the paper is organised as follows. Section 1.1 presents an overview of the steganography types. The proposed framework is explained in Section 3. Experimental results and discussion are given in Section 4. Finally, the paper is summarized in Section 5 with its conclusion and future research outlines.

Steganography (Definition and Types)

The concealment of secret data within a cover object also termed as stego object signifies steganography (Sabah, et al.,2019). Thus, it cannot be detected through this technique, the secret data or retrieved by any intruder that has no authority to do so. The Steganographic technique offers great security and confidentiality (Sabah, et al.,2019; Hashim, et al.,2019). There are six kinds of cover steganography, figure one which is explicated as the following :

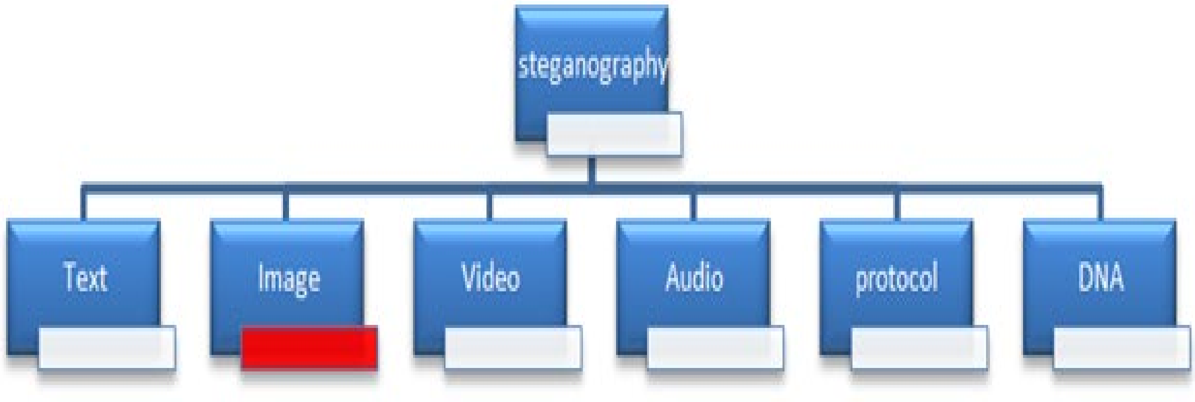
a) **Text**: Within text files, data is concealed. Behind each nth letter of every word in the text message that acts as a cover for hiding the private data. Several techniques are utilised for the concealment of the data within the text file : (i) Format-Based Technique; (ii) Random and Statistical Technique; (iii) Linguistics Technique.

b) **Image**: Image steganography is utilised for the concealment of the data by embedding the secret image into the cover image. The secret image pixel intensity is utilised to hide the data within the cover image. By using digital steganography, the cover source is utilized to insert the secret images through the bits that can be found in digitalised representation of the image.

c) **Audio:** Audio files are used to keep the hiddendata. In order to hide the data, sound files such as WAV, AU, MP3, and others are utilised. There are several techniques involved in audio steganography. The techniques entail (i) LSB (ii) Phase Coding (iii) Spread Spectrum (iv) Echo hiding alongside a review of audio steganography techniques as depicted in Table 1.

d) **Video**: For hiding data, digitized video steganographic method is utilised that consist of a mix of pictures termed as the case video. The DCT modifies the values that are employed in the concealment of the data in individual images within the video that is imperceptible visually. The Video steganography formats can be found in H.264, Mp4, MPEG, and AVI.

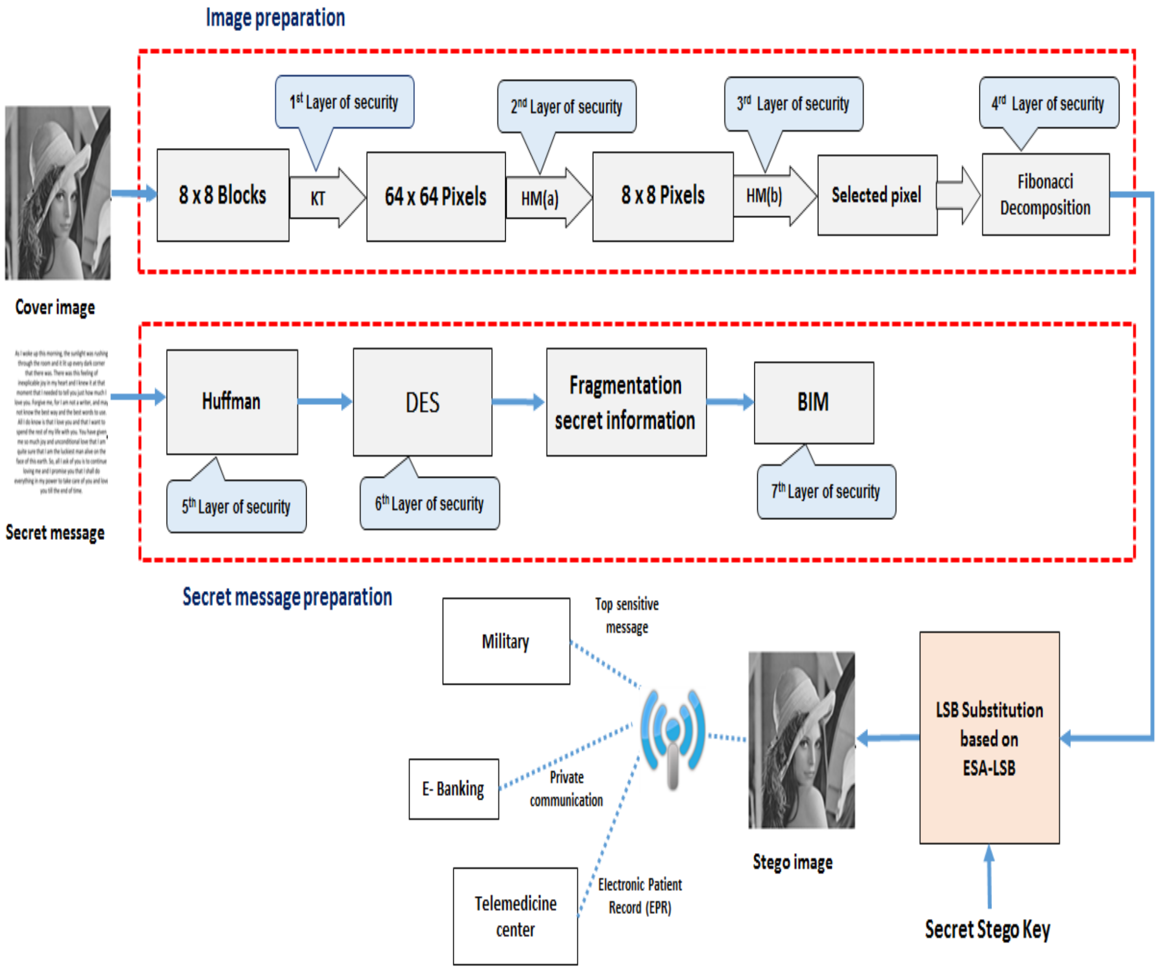
Figure 1. Steganography types



The Proposed Framework

The current section explains the suggested framework graphically with its key modules. Via the graphical framework illustration, the innovative adoptions in the framework are explicated in order that a precise understanding of the image and an insightful comprehension of the recommended scheme could be reached. The recommended scheme that is grounded on the steganographic approach possess multitudinous security layers for images that are in grayscale or colour. Meanwhile, distinct from the alternative steganographic technique which is not able to offer a favourable degree of security, and at the same time, sustain the image quality at a low cost and appropriate payload, that has the ability in keeping the balance among the quality of the image, security, payload and complex computation. The capabilities, possessed by the recommended scheme can be used in the conveyance of a great degree of secret confidential data between the military bodies, electronic banking, wellbeing centres, and other organisations, personal communications which necessitate a high degree of privacy. Figure 2 illustrates a graphic explanation of the recommended scheme.

Figure 2. Public diagram of the presented framework



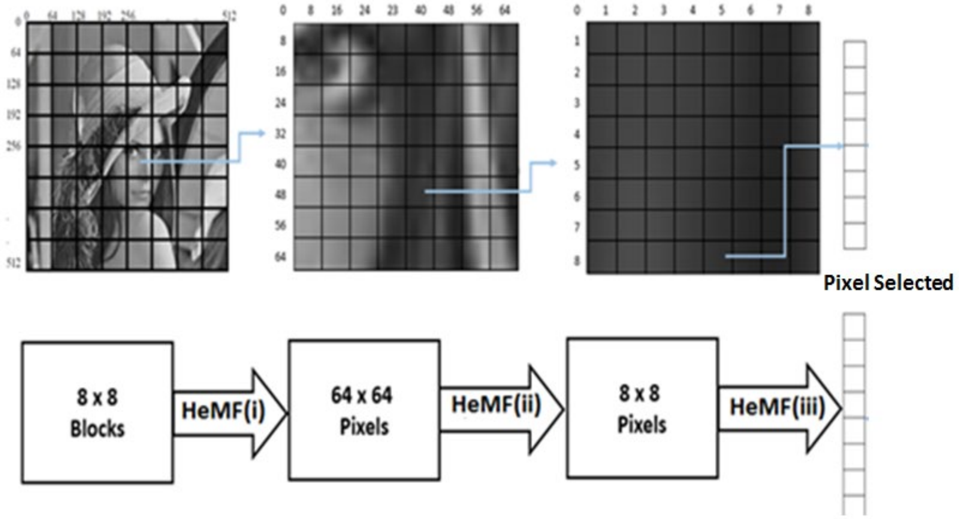
The framework comprises four significant sub-stages that consists of:

i. The readiness of the Image, comprising of the indiscriminate choosing of a pixel according to multi-layers of security.
ii. Getting the secret information ready comprising the secret data being compressed and encrypted before the embedment phase.
iii. The third phase comprises the adjustable concealment of the readied secret information into the cover images via the utilisation of a data embedding algorithm; the procedure facilitates the generation of stego images which can be relayed to respective users.
iv. Finally, the utilisation of the extraction algorithm is used in the extraction of the secret information from the stego image which was sent to the receiver end, and later, the information may be utilised respectively. A short explanation of the four significant stages is provided in the ensuing sections.

Image Preparation

A fundamental aspect of the embedment technique is to determine the pixel needed to conceal the secret data accurately. It is insufficient to determine the embedding site, as it is equally significant to know the following site. Moreover, an additional significant phase is to ascertain the whole course in order that the suggested algorithm is untraceable by everyone, and can only be traced by the recipient or interlocutor. Taking this quality as the foundation, the steganography designers often targets to the utilization of the pixel pathways which are unpredictable by a third party not included in the communication. Taking this into consideration, the utilisation of the multitudinous layer of security alongside with the Henon Map Function algorithm is used in this framework as illustrated in figure 3, in order to improve the achievement of the objectives in offering security, possessing an extremely accurate pixels choice. The image preparation process is executed utilising Henon Map Function (HeMF) algorithm. Using the algorithm, the cover image may be segregated into blocks and sub-blocks up to the point when the pixels were attained. They are overlying each other to ensure the complete embedding of the introduced data, and to guarantee which is nearly improbable to determine the pixels path. Consequently, the security of the suggested framework is ensured.

Figure 3. The presented framework for Random pixel selection



There are three phases in improving the robust nature of the system combating the assaults by the attackers, through the pixels choice. Consequently, it makes it impossible for the attacker to detect the pixel which was initially embedded or the order of the pixels.

Secret Message Preparation

The two essential phases which secret data transients, which are compression and encryption. Following the compression of the data, it will next transient to the following phase, that is the encryption phase. The letters of the alphabets are utilised which randomly produce the secret data at varying lengths.

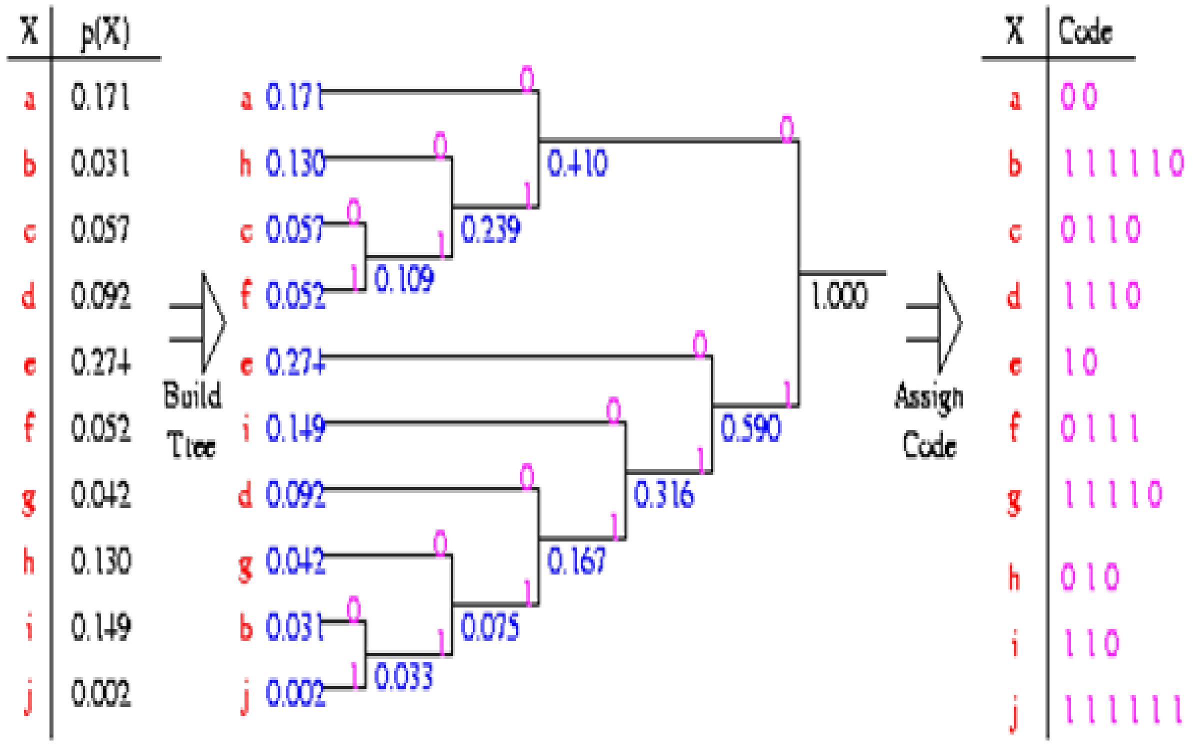
Huffman Compression

Huffman coding is a specific type of prefix code often utilized in lossless data compression. David A. Huffman created an algorithm during his PhD days as a student at MIT, and published "A Method of the Construction of Minimum-Redundancy Codes" paper in 1952 (Khan, et al.,2015).
The general algorithm can be described as:

Input: Alphabet $A = \{a_1, a_2, \dots, a_n\}$ which signify alphabet symbols with size n.
Set $W = \{w_1, w_2, \dots, w_n\}$ which signify positive symbol weight such as $w_i = weight\ (a_i)$, $1 \leq i \leq n$.
Output: Code $C(A, W) = (c_1, c_2, \dots, c_n)$ which are the binary codewords such as c_i is the code words of $a_{i,}$ $1 \leq i \leq n$.
The main **goal** is
Let $L(C) = \sum_{i=1}^{n} w_i \times length\ (c_i)$ is the length of code C with the condition that $L(C) < L(T)$ for any code $T(A, W)$.

Huffman is utilised in the compression of the secret data. However it is improbable to employ for the compression of the image on its own, as it might impact on the concealed data within it, restricting the procedure to solely the secret information flow as illustrated in Figure 4.

Figure 4. Mechanism of Huffman coding algorithm



It can culminate that Huffman coding algorithm is beneficial to the steganographic system to enhance the payload capacity when implemented onto the secret data before embedding. Simultaneously, the robust nature of the system is increased to combat the histogram and statistical attacks.

Bit Inverting Map (BIM)

The recommended framework entails that following the choosing of the pixels, these pixels are arranged into an 8 x 8 pixels sub-window. Ensuring that, every individual pixel's Least Significant Bit is utilised to attain 64 bits, that will be prepared for the embedment procedure.

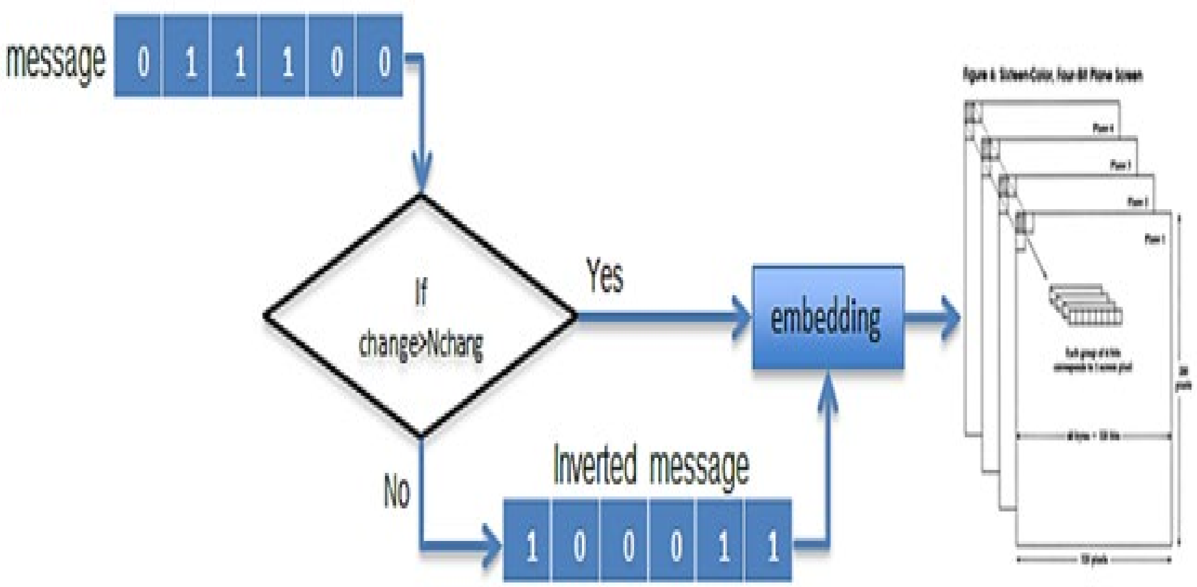
Here, there are 64 bits attained from the image and will be followed by the replacement of 64 bits with 64 bits from the secret data. Furthermore, during this phase, the bit swapping function (BSF) is utilised to check the correspondence between the bits within the original image and the secret data bits. If the corresponding bits quantities are lesser than the unsuitable bits, then the secret data is reversed and embedded. Otherwise, the secret bits must be embedded straight into it. The security layer number seven is obtained by utilising the BSF. Algorithm 1 explicates the operation of bit swapping.

Algorithm 1: Bit Inverting Map

1.	If Bit matched > Bit mismatched then
2.	Embed directly from secret message to image pixel using algorithm 2 Else
3.	Invert the secret message then embed using step 17 in algorithm 2
4.	End if

The incorporation of the embedding algorithm and BIM in the recommended framework is depicted in Figure 5.

Figure 5. Bit Inverting Map method



Embedding Algorithm

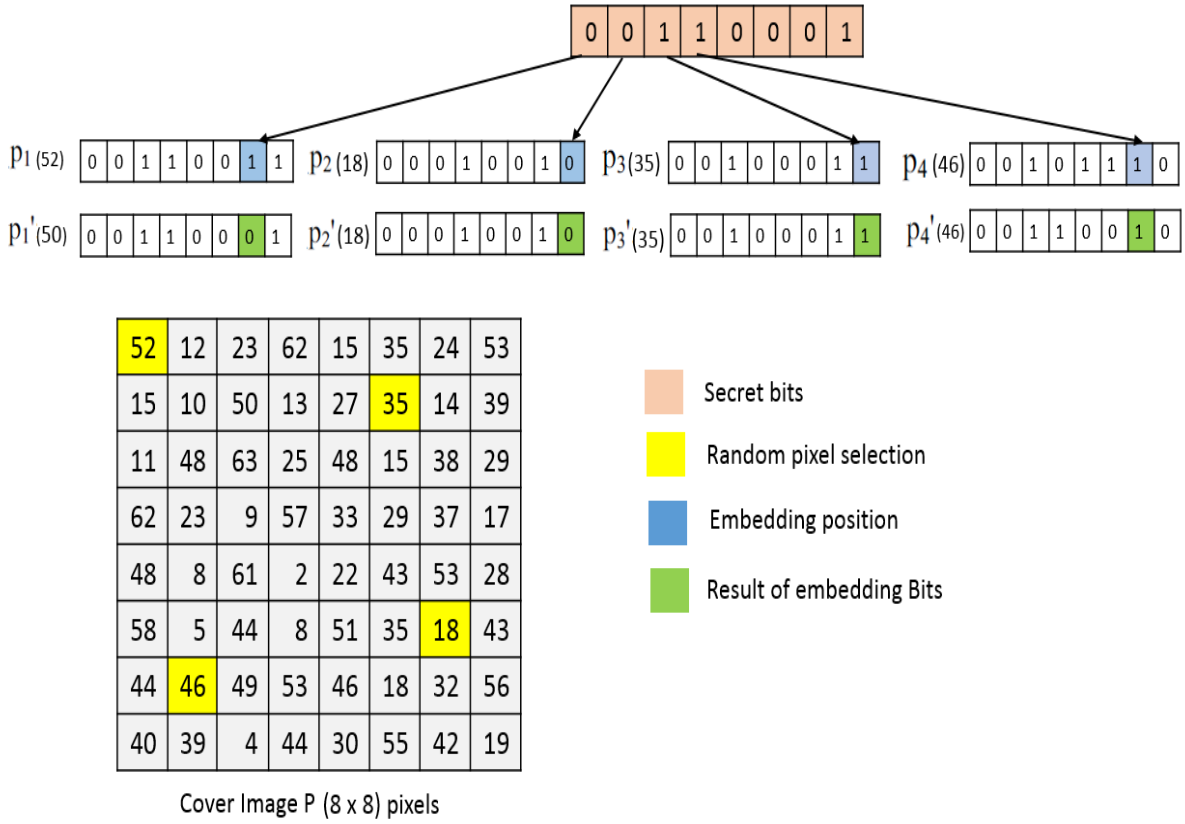
The role of the embedding algorithm is to conceal the secrete data inside a cover image. The embedding algorithm enables the concealment of the data that had undergone encryption and compression inside the Least Significant Bit layer adaptively, assisted by the stego key. In algorithm 2, the important phases entailed with the recommended embedding mechanism are shown. In this method, all the pixels are marked into the block map, and is the utmost critical process; this process is termed as the embedding block.

Algorithm 2: Embedding Algorithm

Input: Cover image (I^m) , Stego key (K^S), Secret Message (M^s).	
1.	Initialize $I^m \longleftarrow$ Cover Image ,$M^s \longleftarrow$ Secret Message , $K^S \longleftarrow$ Stego key
2.	Apply huffman algorithm on M^s to get the compression bit stream (M^{CBS})
3.	Apply DES using algorithm1on M^{CBS} 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^m from dataset of cover images (DS^{CI})
7.	Generate random number 1 and arrange it according to HeMF(i) vector
8.	Select one block of (8 x 8) blocks via HeMF(i) vector
9.	Generate random number 2 and arrange it according to HeMF(ii) vector
10.	Select one sub-block of (64 x 64) pixels via HeMF(ii) vector
11.	Generate random number 3 and arrange it according to HeMF(iii) vector
12.	Select the destination pixel via HeMF(iii) vector
13.	Generate EM vector and arrange it according to (1,0)
14.	Mark the LSB of each pixel and M^{ESI} group
15.	Apply BIM based on algorithm 1
16.	Loop from I=1 : N
17.	Select M^{ESI} bit (0 or 1)
	a. If M^{ESI}=0 and 2-LSB layer is 0, Do no change in 2-LSB layer. b. If M^{ESI}=0 and 2-LSB layer is 1 , Embed in 1-LSB layer via replace 0 to 1-LSB layer. Else if 1-LSB layer is full, Embed in 2-LSB layer. c. If M^{ESI}=1 and 2-LSB is 1, Do no change in 2-LSB layer. d. If M^{ESI}=1 and 2-LSB is 0, Embed in 1-LSB layer via replace 1 to 1-LSB layer. Else if 1-LSB layer is full, Embed in 2-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)	

The clarity of the fundamental idea of the recommended embedding algorithm is shown in the process in Figures 6. Let P be a cover image with pixels [P1, P2, P3, P4], and the secret data readiness that is derived from Section 2.3.1, M^{ESI} = $(00111010)_2$. In order to avert chaos, certain intermediate phases are left out, and the emphasis is given to the main idea.

Figure 6. A general example of embedding for the presented framework



52	12	23	62	15	35	24	53
15	10	50	13	27	35	14	39
11	48	63	25	48	15	38	29
62	23	9	57	33	29	37	17
48	8	61	2	22	43	53	28
58	5	44	8	51	35	18	43
44	46	49	53	46	18	32	56
40	39	4	44	30	55	42	19

Cover Image P (8 x 8) pixels

The attainment of the second goal of this study that is pursued through the recommended scheme is the embedment of the secret data within the Least Significant Bit layer, in order for the maintenance of the image quality such as the original image.

The embedding procedure may be utilised through the ensuing assumptions:

In instances that the second bit of P1 is 0 in LSB and the first bit of M^{ESI} is 0, thus the second LSB layer will be unchanged. For the second pixel P2, in instances, if the second bit is 1 in the Least Significant Bit layer and M^{ESI} bit is 0, substitution will then be made in the first layer of LSB which is 0. For the third pixel P3, in instances when the second bit is 1 in the Least Significant Bit layer and M^{ESI} bit is 1; the second LSB layer is unchanged. For the fourth pixel P4, when the second bit is 0 in the LSB layer and M^{ESI} bit is 1, then substitution occurs in the first layer of the Least Significant Bit which is 1.

As a result, the stego image generates the pixels P1 ′, P2 ′, P3 ′, P4 ′. In this instance, the resultant embedding is depicted by the green colour, while the pixel that is chosen randomly depicted by a blue colour. Moreover, the colour yellow illustrates the secret bits. The Least Significant Bits are transformed during the data embedding procedure.

Extraction Algorithm

The hidden secret data is extracted from the stego image is executed utilising the extraction algorithm. Varying parameters are used for the successful extraction of the secret data. Certain of the parameters consist of the decompression for Huffman coding, the decryption of the (DES), Henon map function (HeMF), Bit Inverting Map (BIM), and the stego key of the data embedding framework. The parameters supported the security feature of the recommended framework, hence enabling it to be robustness so that it is not easy for attackers to retrieve the secret data. The essential phases contained in the recommended mechanism of extraction are illustrated in Algorithm 3.

Algorithm 3: Extraction Algorithm

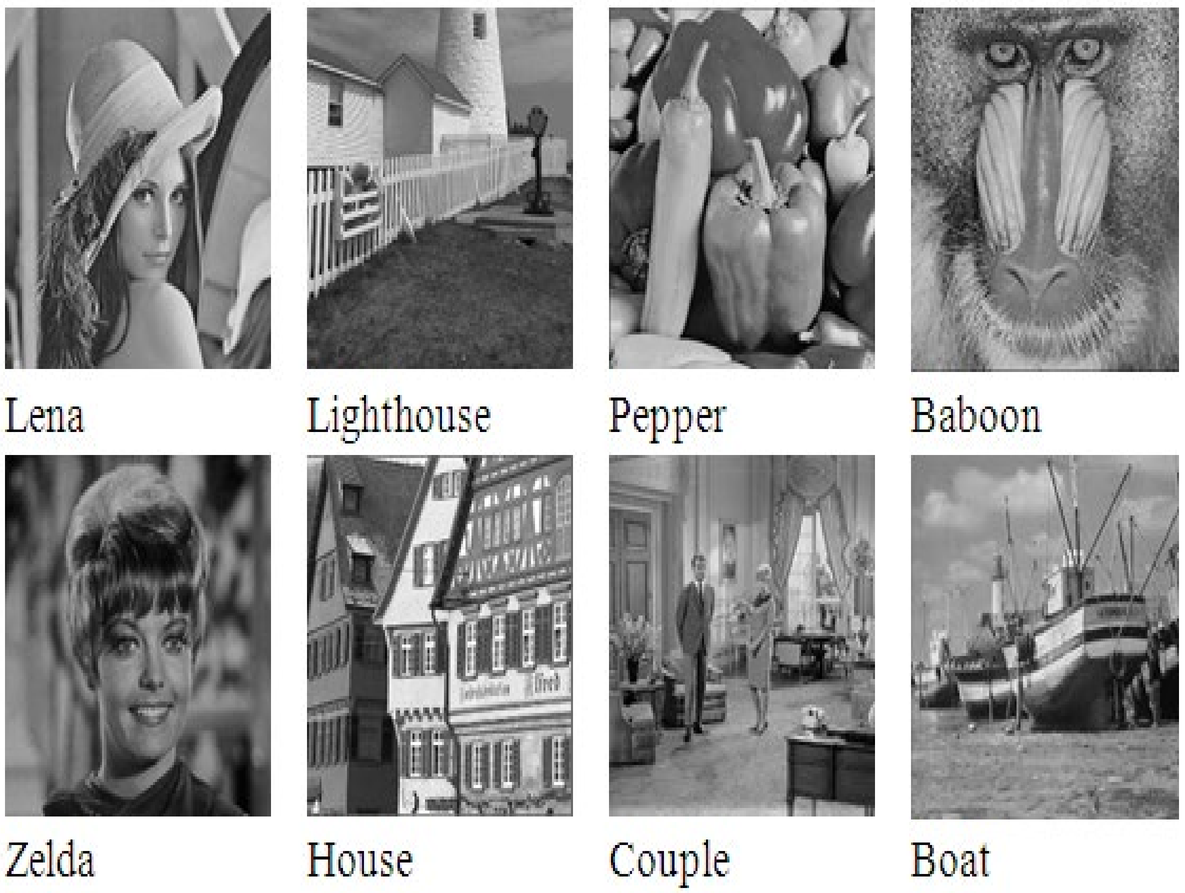
Input: Stego image (I^S) , Stego key (K^S).	
1.	Initialize I^S ⟵ Stego Image , K^S ⟵ Stego key
2.	Apply random number 1 using HeMF(i) vector
3.	Select one block of 64 blocks from HeMF(i) vector
4.	Apply random number 2 using HeMF (ii)vector
5.	Select one sub-block of (64 x 64) pixels from HMF(ii) vector
6.	Apply random number 3 using HeMF(iii) vector
7.	Select the stego pixel from HeMF(iii) vector
8.	Apply EM vector and arrange it according to (0,1)
9.	Mark the LSB of each pixel
10.	Loop from I=1 : N
11.	Reverse the step 17 of embedding process from algorithm 2
12.	Repeat step 11 in algorithm 2, until extract all secret bits from stego image
13.	Reverse the step 15 from algorithm 1
14.	Decrypt the resultant bits using the reverse operation of DES.
15.	Decompression from the resultant bits of step 2 using huffman compression
16.	Re -construct the original data from the achieved bits.
Output: Secret message (M).	

Experimental Results and Discussion

This current study utilised the MATLAB tool with eight standard grayscale images comprised in figure 9 was used. Images with size 512 x 512 were attained from USC-SIPI image database [22]. The outcomes attained took into account the complete capacity of the individual image for the methods mentioned above. The varying stego-images for the recommended method with embedding percentage (EP) = 18.75% are comprised in Figure 7.

The recommended framework was assessed employing parameters such as PSNR, EC, bits per pixel (BPP) and Normalized Cross-Correlation (NCC). To check the robust nature of the recommended scheme in combating attacks, BER and Chi-squared statistical attack were employed.

Figure 7. Cover images used in the presented scheme



Analysis Based on EC, PSNR, BPP, and NCC

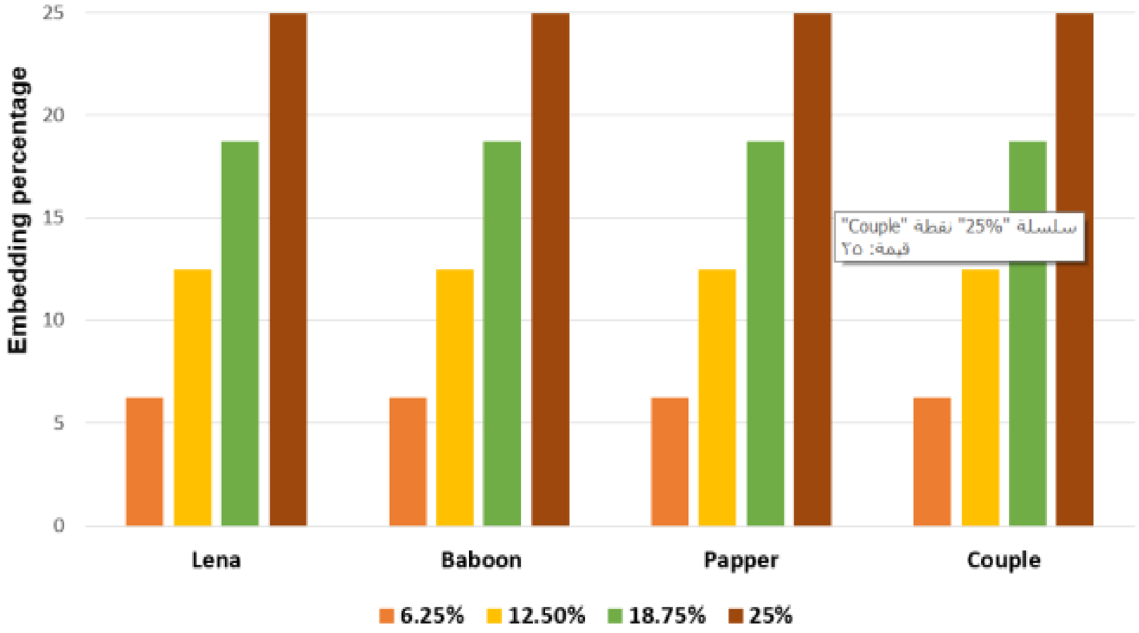
The definition of embedding capacity EC is the ratio of the message bits numbers to the cover pixels numbers (Khan, et al.,2015). It is associated in a direct way with pixel numbers utilised recommended scheme in this study as a varying number of data bits are embedded by a single pixel.

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

This study consists of the employment of varying payload capacities, and shown in percentage form based on the latest studies in this field. Further elucidation is shown as the ensuing given:

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

Figure 8. Various embedding percentages (EP).



The rationale behind why the percentages mentioned above are utilised in the current research stemmed from the varying payloads that were utilised in prior studies, in addition, uniform instruments are needed to attain fair outcomes. The embedding percentages employed in the recommended framework are depicted in Figure 8.

Figure 8. Stego-images (a–h) for the proposed framework for EP = 18.75%

a- Lena b- Lighthouse c- Pepper d- Baboon

e- Zelda f- House g- Couple -Boat

Human Visual System (HVS) or Human Audio System (HAS) is the features that are taken into consideration for the acquisition of imperceptibility, in order that there will be absence of perceptible artifacts that remain, so that human beings are not able to distinguish between the cover with concealed data and the cover with no concealed data [Khan, et al.,2015]. The technique for image quality assessment is ascertained by peak signal to noise ratio (PSNR), that is computed following the embedding procedure for the comparison between the original and stego images. The embedding of data is perceived as not being perceptible to the human vision system (HVS), in the case that the outcome of the PSNR calculation is equal to or greater than 30db [Tayarani-N, and Mehdi,2015]. Through the application of the following equations, the PSNR is computed.

$$PSNR = 10log_{10}\left(\frac{255^2}{MSR}\right) \qquad (5)$$

Where, the MSE is mean square error, that is calculated through the equation :

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

Where, m and n are the sizes of the images, and while x and y are the cover and stego images accordingly. At the time of executing the recommended framework, two significant phases were conducted in this research, which is the training and testing phases. In the typical image processing, the stego image imperceptibility is gauged by utilising PSNR measures (Tayarani-N, and Mehdi,2015). Through the application of the PSNR measures as aforementioned, the stego image fidelity is assessed against the original carrier image. Moreover, the degree of stego image deformation is gauged against the carrier image; where the measurement is in decibel (dB). In instances where a higher score of PSNR is attained, it signifies that the image quality is great, hence keeping the possibility of being of detected to a minimal utilising the HVS. Via the training phase, the PSNR magnitude is inversely proportional to the MSE, signifying the increase in the mismatch between the original image and stego message. In circumstances when the MSE is huge, the outcome will be not favourable in terms of PSNR due to its functioning as aforementioned in equation (PSNR). The issue was resolved in the testing stage and the outcome displayed a better achievement in comparison to alternative methods. The BPP provides the average number of bits which can be concealed per pixel (Hemrajani, and Anil,2013). The outcomes from the experiments for the recommended framework, and the methods of Kumar and Chand (Arch-Int, and Ngamnij,2016), Yang (Quan, et al.,2015), Mohammed et al. (Mohd Rahim, and Mohd Shafry,2017), Chunget al. (Wen-Chung, et al.,2017), are illustrated in tables 1, and. Furthermore, comparisons of the said methods and recommended framework were carried out according to PSNR, EC and BPP accordingly.

Image (512 x 512)	Proposed Scheme (6.25%)					Proposed Scheme (12.5%)				
	PSNR	EC	BPP	FOBP	SSIM	PSNR	EC	BPP	FOBP	SSIM
Lena	72.90	131,062	0.5	0	1	66.63	265,144	1.0	0	0.98
Lighthouse	72.90	131,062	0.5	0	1	66.62	265,144	1.0	0	0.98
Zelda	72.87	131,062	0.5	0	1	66.66	265,144	1.0	0	0.98
Pepper	72.63	131,062	0.5	0	1	66.63	265,144	1.0	0	0.98
Baboon	72.87	131,062	0.5	0	1	66.69	265,144	1.0	0	0.98
Boat	72.63	131,062	0.5	0	1	66.68	265,144	1.0	0	0.98
House	72.88	131,062	0.5	0	1	66.64	265,144	1.0	0	0.98

Couple	72.90	131,062	0.5	0	1	66.63	265,144	1.0	0	0.98
Average	**72.82**	**131,062**	**0.5**	**0**	**1**	**66.64**	265,144	1.0	**0**	**0.98**

Table 1: Results for the proposed scheme with 6.25% and 12.5% of EP

The PSNR of the proposed technique for embedding percentage EP= 6.25% is 72.82 dB, for EP = 12.5% it is 66.64 dB, for EP = 18.75 it is 61.17 dB, and for EP = 25% it is 54.93 dB. Similarly, the EC of the proposed technique is 131,072, 265,144, 393,216 and 524,288 bits for EP = 6.25%, 12.5%, 18.75 and 25% respectively.

Table 7: Results for the proposed scheme with 18.75% and 25% of EP

Image (512 x 512)	Proposed Scheme (18.75%)					Proposed Scheme (25%)				
	PSNR	EC	BPP	FOBP	SSIM	PSNR	EC	BPP	FOBP	SSIM
Lena	61.15	393,216	0.5	0	0.99	54.90	524,278	2.0	0	0.98
Lighthouse	61.15	393,216	0.5	0	0.99	54.90	524,278	2.0	0	0.97
Zelda	61.15	393,216	0.5	0	0.99	54.91	524,278	2.0	0	0.98
Pepper	61.28	393,216	0.5	0	0.99	55.15	524,278	2.0	0	0.98
Baboon	61.13	393,216	0.5	0	0.99	54.92	524,278	2.0	0	0.98
Boat	61.14	393,216	0.5	0	0.99	54.90	524,278	2.0	0	0.97
House	61.15	393,216	0.5	0	0.99	54.91	524,278	2.0	0	0.98
Couple	61.17	393,216	0.5	0	0.99	54.91	524,278	2.0	0	0.97
Average	**61.16**	393,216	0.5	**0**	**0.99**	**54.93**	524,278	2.0	**0**	**0.98**

Conclusion

The current study consisted of a recommendation of new secure image steganography framework that termed as an adaptive stego key LSB (ASK-LSB) framework, in accordance to four stages to enhance the data-hiding algorithm in cover images through the utilisation of the capacity, quality of image, and security.

The secure image steganography framework, which is recommended in the current research, is founded on a new adaptive LSB substitution technique, random function, DES algorithm, and Huffman compression algorithm.

The utilisation of the adaptive LSB substitution technique involves the embedment of the secret data inside a cover image, according to the stego key. The randomness enables the system to be more robust in combating unauthorised entities attempting to uncover the choice of pixel to make the initial embedment or the pixels order series. The encryption procedure implementation for the secret data is to produce secret data with a binary equivalent random sequence, which obstructs attacks to the secret data. Payload capacity was employed with this research, and is manifested in the form of a percentage in accordance with researchers found in the latest studies. The recommended work entails the straight insertion of secret bits or inverse insertion, that improves the complicatedness and imperceptible nature of the embedding procedure. The algorithm has offered a multitudinous layer of a security operating cooperatively to enhance protection against attacks. The hiding algorithm was recommended to combat two kinds of attacks: which are visual and statistical attacks.

REFERENCES

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.

Aragon, Nicolas, et al. "Low Rank Parity Check Codes: New Decoding Algorithms and Applications to Cryptography." *arXiv preprint arXiv:1904.00357* (2019).

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.

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.

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

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.

Choudhary, Kaustubh. "Image steganography and global terrorism." *International Journal of Scientific & Engineering Research* 3.7 (2012): 1-12.

Fyffe, Blair, Yunjia Wang, and Ishbel Duncan. "Human visual based perception of steganographic images." *Journal of Cyber Security Technology* (2019): 1-47.

Zhang, Yi, et al. "Multiple Robustness Enhancements for Image Adaptive Steganography in Lossy Channels." *IEEE Transactions on Circuits and Systems for Video Technology* (2019).

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* 40.5 (2016): 114.

Lee, Yen-Po, et al. "High-payload image hiding with quality recovery using tri-way pixel-value differencing." *Information Sciences* 191 (2012): 214-225.

Sahu, Aditya Kumar, and Gandharba Swain. "An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function." *Wireless Personal Communications* (2019): 1-16.

Modi, Mangat Rai, Saiful Islam, and Phalguni Gupta. "Edge based steganography on colored images." *International Conference on Intelligent Computing*. Springer, Berlin, Heidelberg, 2013.

Rengarajan Amirtharajan, K., A. Kingsly Infant, and J. B. B. Rayappan. "High performance pixel indicator for colour image steganography." *Information Technology* 5.3 (2013): 277-290.

Chen, Jeanne. "A PVD-based data hiding method with histogram preserving using pixel pair matching." *Signal Processing: Image Communication* 29.3 (2014): 375-384.

Rabie, Tamer, Ibrahim Kamel, and Mohammed Baziyad. "Maximizing embedding capacity and stego quality: curve-fitting in the transform domain." *Multimedia Tools and Applications* 77.7 (2018): 8295-8326.

Rabie, Tamer, Mohammed Baziyad, and Ibrahim Kamel. "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid." *Multimedia Tools and Applications* 77.18 (2018): 23673-23698.

Kanojia, Pallavi, and Vijay Choudhary. "LSB Based Image Steganography With The Aid of Secret Key and Enhance its Capacity via Reducing Bit String Length." *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2019.

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

Zhu, Zhenhao, Tao Zhang, and Baoji Wan. "A special detector for the edge adaptive image steganography based on LSB matching revisited." *2013 10th IEEE International Conference on Control and Automation (ICCA)*. IEEE, 2013.

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

Cheng, Wei-Chung, and Massoud Pedram. "Chromatic encoding: A low power encoding technique for digital visual interface." *IEEE Transactions on Consumer Electronics* 50.1 (2004): 320-328.

Muhammad, Khan, et al. "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption." *TIIS* 9.5 (2015): 1938-1962.

Aziz, Mahdi, Mohammad H. Tayarani-N, and Mehdi Afsar. "A cycling chaos-based cryptic-free algorithm for image steganography." *Nonlinear Dynamics* 80.3 (2015): 1271-1290.

Ramaiya, Manoj Kumar, Naveen Hemrajani, and Anil Kishore Saxena. "Security improvisation in image steganography using DES." *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013.

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* 75.14 (2016): 8319-8345.

Liu, Quan, et al. "A novel image encryption algorithm based on chaos maps with Markov properties." *Communications in Nonlinear Science and Numerical Simulation* 20.2 (2015): 506-515.

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).

Kuo, Wen-Chung, et al. "Secure multi-group data hiding based on gemd map." *Multimedia Tools and Applications* 76.2 (2017): 1901-1919. Falah.Y.H.Ahmed,Muthukumaran a/l Thiruchelvam, and Muhammad Irsyad Abdullah (2019). Improvement of Vehicle Management System (IVMS). IEEE International Conference on Automatic Control and Intelligent Systems, Scopus .

Dhafer Sabah Yaseen, Shamala A/P Batumalai, Falah Y H Ahmed and Sim Liew Fong (2019). Improved Disabled Mobile Aid Application for Android : Health and Fitness Helper for Disabled People. 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC), Scopus.

Falah.Y.H.Ahmed,Muthukumaran a/l Thiruchelvam, and Muhammad Irsyad Abdullah (2019). Improvement of Vehicle Management System (IVMS). IEEE International Conference on Automatic Control and Intelligent Systems, Scopus .

Dian Nugraha and Falah Y. H. Ahmed (2019). Advancement parking application using MEAN stack: A narrative review (FIRST 2018 Conference in Palembang Indonesia Scopus.

Sim Liew Fong, Amir Ariff Azham bin Abu Bakar, Falah Y.H Ahmed, Arshad Jamal (2019). Smart Transportation System Using RFID (Proceedings of the 2019 8th International Conference on Software and Computer Applications) publisher ACM 579-584. Scopus.

Sim Liew Fong, David Chin Wui Yung, Falah YH Ahmed, Arshad Jamal (2019). Smart City Bus Application with Quick Response (QR) Code Payment (Proceedings of the 2019 8th International Conference on Software and Computer Applications) publisher ACM 248-252. Scopus.

Falah Y.H. Ahmed, Omar Ahmed Mahmood, Ahmed Sabeeh Yousif (2019). Comparison between improved histogram shifting and LSB (bit-plan mapping) in digital watermarking techniques (International Journal of Engineering & Technology) Science Publishing Corporation, Pages5322-5326 /4/7. Scopus.

Dian Nugraha and Falah Y. H. Ahmed (2019). MEAN stack to enhance the advancement of parking application: A narrative review. IOP science (Journal of Physics: Conference Series) 1088/1742-6596/1167/1/012075,V 1179.
Scopus.

Falah Y.H. Ahmed & Siti Mariyam Shamsuddin (2019). Spikeprop Deep Learning with Multiple Weights Optimization of Differential Evolution and Particle Swarm Optimization (Hindawi Publishing journal of Computational Intelligence and Neuroscience) 7547924 in ISI Impact Factor 0.430.