Multimedia Tools and Applications (2022) 81:25913–25946
https://doi.org/10.1007/s11042-022-12691-9

High payload image steganography scheme with minimum distortion based on distinction grade value method

Mustafa Sabah Taha [1,2] · Mohd Shafry Mohd Rahem [1] · Mohammed Mahdi Hashim [1,3] · Hiyam N. Khalid [4]

Received: 29 October 2020 / Revised: 31 March 2021 / Accepted: 21 February 2022 /
Published online: 25 March 2022

Abstract
Presently, the design and development of an effective image steganography system are facing several challenges including the low capacity, poor robustness and imperceptibility. To surmount such limitations, it is important to improve the capacity and security of the steganography system while maintaining a high signal-to-noise ratio (PSNR). Based on these factors, this study is aimed to design and develop a distinction grade value (DGV) method to effectively embed the secret data into a cover image for achieving a robust steganography scheme. The design and implementation of the proposed scheme involved three phases. First, a new encryption method called the shuffle the segments of secret message (SSSM) was incorporated with an enhanced Huffman compression algorithm to improve the text security and payload capacity of the scheme. Second, the Fibonacci-based image transformation decomposition method was used to extend the pixel's bit from 8 to 12 for improving the robustness of the scheme. Third, an improved embedding method was utilized by integrating a random block/pixel selection with the DGV and implicit secret key generation for enhancing the imperceptibility of the scheme. The performance of the proposed scheme is assessed experimentally to determine the imperceptibility, security, robustness and capacity. The resistance of the proposed scheme is tested against the statistical, χ^2, Histogram and non-structural steganalysis detection attacks. The obtained PSNR values revealed the accomplishment of the higher imperceptibility and security by the proposed DGV scheme while maintaining higher capacity compared to the reported findings. In short, the proposed steganography scheme outperformed the commercially available data hiding schemes, thereby resolved the existing issues.

✉ Mustafa Sabah Taha
timimymustafa@gmail.com

[1] School of Computing, Facility of Engineering, University Technology Malaysia, Johor Bahru, Malaysia

[2] Missan Oil Training Institute, Ministry of Oil, Baghdad, Iraq

[3] Technical Engineering College, Middle Technical University, Baghdad, Iraq

[4] Imam Al - Kadhim University for Islamic Sciences, Baghdad, Iraq

Keywords Information security · Data hiding · Image steganography · Image visual quality · LSB · Fibonacci decomposition

1 Introduction

In the internet era, sending and receiving data and information in the form of video, audio, image, and text become very easy. However, such easy access to the vast amount of information has posed severe threats to the security and privacy of the data. As such, securing the information over the non-secured public network is challenging. Often, the unauthorized users, intruders, attackers or adversaries can corrupt the information by manipulating the message, causing financial or ethical damages. Thus, to attain the secured data communications various information encryption and hiding schemes have been developed.

The term steganography refers to the method of hiding sensitive data inside a trusted media and then transmitting that hidden data over the Internet through reliable media without noticing or discovering by the human eyes. So that it becomes unnoticed by hackers or unauthorized users [26]. The term steganography is derived from two Greek words, "Stegos" and "grafia", which means "cover" and "writing", hence it is literally defined as "cover writing" [21, 24]. It can be categorized into several types depending on the cover medium including the image, audio, text, video, DNA or even protocol. Each of these cover media has its advantage and drawbacks [18, 21]. Among these media, images are mostly used as a cover media due to their availability, easy usage by the users, high capacity and imperceptibility [49].

Over the last decade, many research efforts have been dedicated to develop Image Steganography Systems (ISSs). These systems gained the popularity due to the easy communication of the multimedia content through low-cost devices like mobiles and IP cameras, and social media like WhatsApp, Twitter, and Facebook [18]. In addition to the understanding of the secret data embedding in an image, several issues involving the image security and hiding of the secret message still remain unsolved [15, 53].

Various terminologies are used to refer to the mechanism of using image steganography systems. *Cover image* is the original image without any hidden bits (image before embedding); while *Stego image* is the image that hosts the secret bits with a certain quality (image after embedding); Whereas concealment protocols (the necessary information of hiding and extracting process) are saved in a shared key between the sender and the receiver party called a *Stego key.* Finally, the *Secret data* can be a simple text message, image, video, or audio. In short, there are two aspects of this descriptions, the sender needs to hide the message and the receiver needs to extract the hidden message from the stego image via the information stored in the stego key. Therefore, the main aim of the image steganography is to maintain the stego image and then receive it without being noticed by the intruders or attackers [36]. The schematic diagram in Fig. 1. depicts the working principle of a typical steganography model.

The robustness of a steganographic model depends on the suitability of the embedding process of the secret message in the cover image [29]. The presence of any fault in certain steganography stage makes the scheme less secured [49]. A successful steganography system must support high capacity to carry more information, enhancing the security to make the system highly secured and reliability to ensure the imperceptibility of the system [18]. Furthermore, the imperceptibility determines the robustness of the steganography system [40]. It is important to note that hackers are aware of the most of the existing steganography methods [21]. Thus, it is obligatory to devise a new steganography scheme with cutting-edge

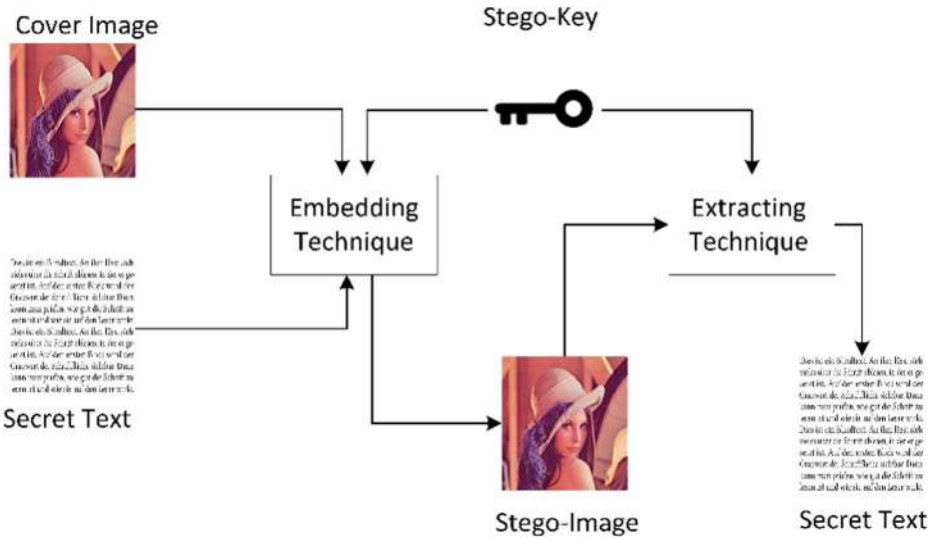

Fig. 1 A block diagram of steganography model

ideas so that they become less susceptible to the attacks. To this end, this study focuses on an improved embedding process for both secret message and cover image, which increases the capacity, imperceptibility and robustness of the proposed steganography scheme.

Figure 2 shows fundamental features of an ISSs and the associated problems that need to be addressed. The challenges of the existing image steganography methods and limitations concerning the embedding solutions are emphasized [6, 20, 23, 32, 58, 59]. The highlighted requirements must be fulfilled during the design of the image steganography scheme. An ISSs with excellent security, high payload capacity and accurate embedding process have been deficient. In addition, the security of the secret message and payload capacity of the hidden data inside the stego image need to be enhanced. The embedding method must be able to improve the imperceptibility, wherein a new random partitioning technique can be used to enhance the robustness of the proposed scheme. The security performance of any steganography method is determined by the amount of data hidden in the stego image. To maintain highly secured stego image, existing works tend to reduce the data embedded into it [22]. The intuition is that, the steganography developers try to keep the stego image as original as possible [9, 39]. However, such approach adversely affects the capacity of the stego image, and consequently, limits the ability of the steganography system to only embed small amount of data into the cover image. As such, any proposed solution needs to increase the imperceptibility while maintaining high capacity.

Although, many encryption methods have been suggested in the literature to improve the security of the payload, these methods are susceptible to cryptanalysis attacks. This is because these techniques rely on the changes in the order of bits, letters, or words which in turn

Table 1 The generated random key for the Hénon map

0.323
0.210
0.986
0.763

depends on the random number generators to generate the encryption key [3, 48]. Fundamentally, the random number generators are used to produce the encryption key used to encrypt the secret text. Usually, two types of random number generators are utilized including the True Random Number Generator (TRNG) and Pseudo-Random Number Generator (PRNG). The TRGN relies on entropy as a non-deterministic approach to implement the randomness. This gives the TRGN the ability to generate a difficult-to-break encrypted text. However, the TRNG is a time-consuming technique, which makes non-practical when dealing with large size of the text [12]. This means the TRNG technique requires a long encryption key, which in turn occupies more space from the vector which is responsible for carrying the encryption information in the stego image. Additionally, TRNG can be statistically analyzed, which facilitates decoding the cypher text.

The primary aim of an efficient image steganography system is to send the maximum amount of data using the minimum pixels of the cover media. It enables reducing the interception probability while sending through an insecure channel and thereby demands high embedding capacity. According to Nyeem [37], the embedding rate is the amount of hidden data (in bits) compared to the original image size. Keeping higher payload capacity without sacrificing the imperceptibility and security is a major challenge in the steganography system development [21].

One of the prerequisites of any message embedding process is the imperceptibility which hides the secret bits in the digital image so that it remains invisible to the naked eye or statistics [42]. The embedding process is inherently related to the payload volume of the secret data and security of the steganography system. Therefore, any reduction in the embedded data to the cover image can make little alteration of the bits in the original image. This keeps the stego image almost similar to the original image [17, 25]. The image quality of a steganography method is evaluated using the peak signal to noise ratio (PSNR) measure [31]. The PSNR value is calculated by comparing the original and stego images after performing the embedding process. The data embedding process is considered to be imperceptible to the human vision system (HVS) if the PSNR value is greater than or equal to 30 dB [7]. A pixel expansion reversible data hiding (PE-RDH) method with a high EC and good stego-image quality are proposed by Anushiadevi et al. [8]. The proposed PE-RDH method was based on three typical RDH schemes, namely difference expansion, histogram shifting, and pixel value ordering. Compared with another methods, the approach achieved better results in terms of its EC, location map size and imperceptibility of directly decrypted images.

A new efficient embedding algorithm in the wavelet domain of digital images based on the diamond encoding (DE) scheme has been presented by Atawneh et al. [10]. The proposed algorithm first converts the secret image into a sequence of base-5 digits. After that, the cover image is transformed into the DWT domain and segmented into 2×1 coefficient pairs. Abd El-Latif et al. [1] proposed new quantum information hiding approaches are put forward and showed that the quantum secret image was encrypted first using a controlled-NOT gate to demonstrate the security of the embedded data. In another respect, a new color image processing tool termed as the quaternion Hadamard transform is proposed by Li et al. [28] and reported that the proposed color image watermarking is not only invisible but also robust against a wide variety of attacks. In order to ensure the robustness and security of digital image watermarking, Li et al. [27] propose a novel algorithm using synergetic neural networks. The findings showed that the proposed model obtains an optimal Peak Signal-to-noise ratio (PSNR) compared with other models. Abdulla [2] developed some image procedures and

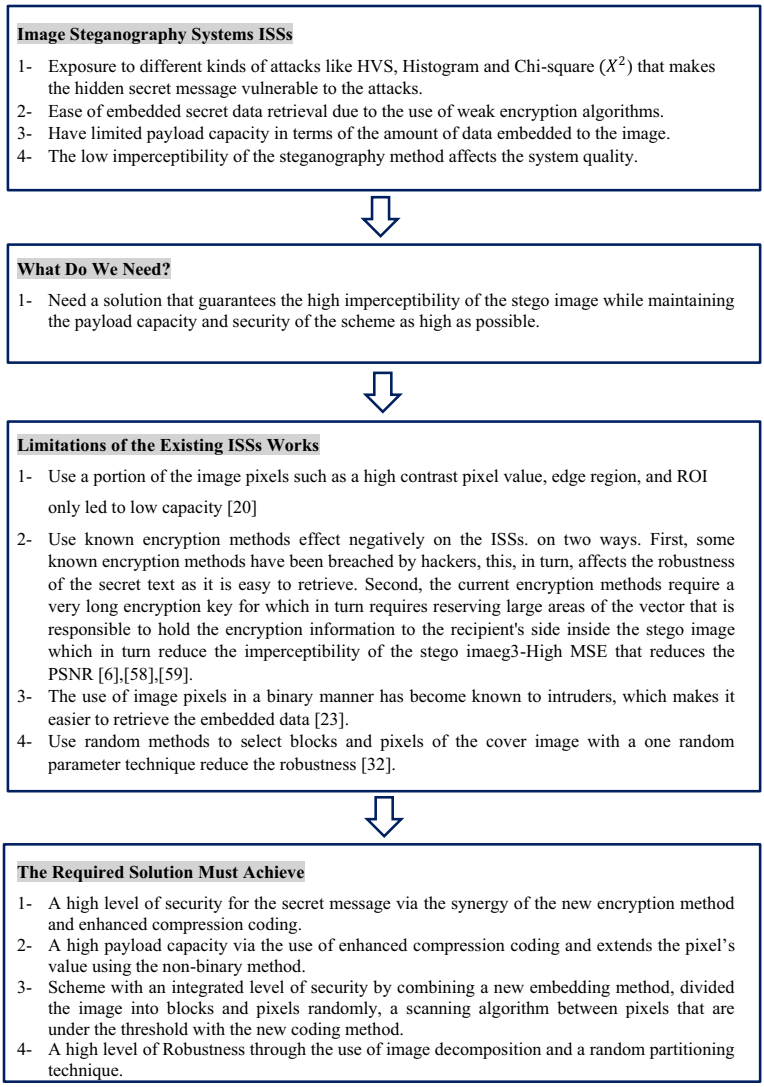

Fig. 2 The problems that need to be addressed and resolved in the existing ISSs

models that increase the similarity between the cover image LSB plane and the cover image bit-stream.

Over the past decades, the developers of the image steganography and steganalysis have paid much attention to enhance the PSNR value during the evaluation of the image steganography system [55]. Although different proposed techniques improved the PSNR, they could not maintain an acceptable level of the payload capacity [44, 45]. Thus, an accurate embedding method is still required to maintain the trade-off between security and imperceptibility of the stego image and increase the robustness of the steganography system. Few studies have been tried to reduce the value of the mean square error (MSE) for the embedding process to enhance the PSNR values [4]. However, this comes at the cost of imperceptibility of the stego image, and consequently the robustness of the steganography system.

According to the above survey, there is a need to address this issue and by building a robust steganography method that guarantees the security, capacity, imperceptibility of the stego imag. Therefore, this study uses images as the cover media to host the text as a secret message. Image steganography can be used in an enormous range of applications such as safe circulation of vital data in an intelligence, e-voting security, e-money security, military, industry, health care, habitat and cloud computing.

2 Literature review

The majority of the earlier investigations on the image steganography system used proficient and organized protocols. In the past, the works on the information concealing generally tried to understand the entire concept regarding the central domain. Then, the focus was shifted to the image steganography systems due to their several benefits compared to other kinds of information hiding protocols such as the text-based or audio-based steganography systems. Thus, it is customary to critically overview in-depth the past development on the digital image steganography systems that dealt with the varieties of applications as well as the performance evaluation criteria used for the hosted image. Briefly, an all-inclusive overview of the relevant literature in the domain of the image steganography systems has been emphasized. This, in turn, substantiated the primary aims and objectives of this study together with the raised questions depending on the appropriate research gaps. In this section, the authors rely on a critical review of relevant techniques and methods to identify the scientific gap and then contribute to proposing a new method capable of resolving these limitations.

A steganography system based on the pixel difference value (PDV) was introduced by Wu et al. [56]. The difference value between two neighbouring pixels was used to determine the number of secret bits that can be embedded. The main issue of this technique is related to the selection of the difference in the pixel value often called contrast or variance. Generally, the image pixels contain two values such as the grey and colour. The grey pixel encloses 8-bits in a one dimensional array [46]. Conversely, the color pixel is coded as RGB pixel value [29], using three vectors of pixels storage that need (3×8) bits to become 24 pixels. The PVD method usually embeds the larger secret bits into the images with higher visual imperceptibility, implying that the image has more different contrast especially with the grey image than the LSB substitution method. Consequently, the PSNR value remains above 40 dB and can bypass the RS detection attacks. The other issue of the PVD method is connected to the histogram that reveals the existence of the secret bits. The falling-of-boundary procedure is one of the significant problems. In the method, the general image contains a smoother area instead of high texture, thus the secret data bits can be hidden in the range of small value. Figure 3 depicts the PVD-based embedding procedure.

In this technique, the high quality image is introduced as the stego image to achieve enhanced payload capacity for hiding the data. The embedding is performed at the edge of the smooth areas where the pixels with neighbors have high intensity variations. Any modification in the smooth area of the image becomes noticeable by an individual's eye. Thus, the smooth area can be neglected while most of the embedding can occur at the edge area where the intensity of the pixel has big differences (called the less sensitive area). The target pixel that needs to be embedded must check its surrounding pixels to ensure the suitable position of the pixel in the image. The surrounding pixels have the probability to find the up p (x, y-1), down p (x, y + 1), right p (x + 1, y) and left p (x-1, y) pixels for the given pixel

p(x,y). The main advantage of this procedure is the accomplishment of the high capacity with improved image peculiarity due to the non-arbitrary changes of the pixels. In addition, the security becomes improved because of the non-sequential embedding that may happens in the 3-bitplance and depends on the pixels' intensity calculation.

Grajeda et al. [16] suggested an image steganography system using the Pixel-Value Differencing (PVD) embedding method and achieved the PSNR of 40.44 dB. However, it failed to uplift the score. Another steganography system based on PVD method of embedding secret message was proposed by Mukherjee et al. [32] that achieved an acceptable PSNR value of 42.66 dB with a reasonable imperceptibility and average bit error rate (BER) of 1.47. A steganography method was proposed [51] in two variants using the combination of the PVD technique and modified LSB substitution. The first variant operated on 2 × 3 pixel blocks and the second one operated on 3 × 3 pixel blocks. The embedding was performed in one of the block pixels using the modified LSB substitution. Based on the new value of this pixel, the difference values with other neighboring pixels were calculated. Using these differences, the PVD approach was applied. The edges in the multiple directions were exploited, so that this steganography became undetectable by the PDH analysis. The LSB substitution was performed in only one pixel of the block. Recently, a new method based on the PVD system has been proposed by Swain [38, 52]. It used two PVD methods with 1 × 2 pixel blocks in an overlapped manner. The first method used an adaptive quantization range table and modular arithmetic for embedding and extraction. The second method used a fixed quantization range table and addition/difference mechanism for the embedding and extraction processes. The method gained a PSNR value of 39.51 that reflected the poor imperceptibility with the payload capacity of 300 KB. Later, some different embedding methods have been suggested by Sahu and Swain [43], for hiding the secret message into the gray cover images. The cover image was divided into blocks according to the sensitive and non-sensitive pixels and the intensity for each block was calculated. This method achieved high imperceptibility.

2.1 The proposal research framework

This paper aims to develop a robust steganography scheme for concealing the messages in the host images for various image sizes/dimensions. The secret messages will be analysed and prepared for embedding into the given image. The image will be formatted logically in 12-bit planes. The last bit plane will be used to embed the secret message in the Least Significant Bit (LSB) that makes a slight alteration in the image quality. Thus, the main contribution of this study is related to the embedding of the secret message in pixels with less difference in the value. In addition, the secret message will be encrypted in the pre-processing stage before the

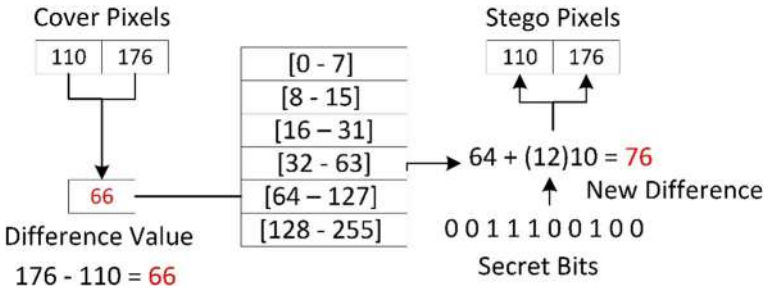

Fig. 3 The basic mechanism of the PVD method

compression. Practically, the secret message will be embedded in an image using a random function generation method together with a novel embedding technique. Consequently, this stage made the stego-image identical to the original image, thereby ensuring the imperceptibility. Furthermore, the secret message will be extracted from the stego-image that was performed in the receiver end. Finally, the performance of the proposed steganography scheme will be evaluated using various metrics including the PSNR, MSE, NCC, SSIM, HVS attack, Histogram attack and X^2 attack. Fig. 4 illustrates the general research framework of this study indicating the detail procedure to accomplish the research goal.

2.2 Data pre-processing

The pre-processing stage is the most vital part of the proposed steganography scheme for achieving an improved security of the secret message and the payload capacity. Thus, two important processes occur simultaneously at this stage including the preparation of the secret message and cover image.

2.2.1 Secret message pre-processing

The pre-processing stage of the secret message was performed before the embedment which is vital for any digital steganography system. The pre-processing of the secret message involves two stages such as the text encryption and compression. The idea behind the pre-processing of the secret message enables to add an extra level of the security on top of increasing the payload capacity of the hidden bits. In the previous studies, the researchers have used different payload capacities to be hidden in a digital image [19, 30, 57]. Consequently, the hidden payload capacities were differed in terms of the pre-processing from one researcher to another. To overcome such limitation, the current study has a new encryption method based on three parameters (to increase complexity) called shuffle the segments of secret message method (SSSM) was suggested for the first time. Furthermore, to accomplish a good embedding capacity the Huffman algorithm was enhanced and applied to the secret message before the embedding wherein the use of such algorithm allowed compressing the secret text more securely and efficiently.

2.2.2 Shuffle the segments of secret message method (SSSM)

The SSSM is used to encrypt the vital data in order to add a new level of security and make its extraction from the stego image intricate for intruders or attackers. It is relatively light-weight compared to DES, AES, and other complex algorithms [14].which is its motivational purpose of choosing. It consists of three victors were designed and associated with three parameters generated sequentially in an iterative fashion (where one was based on another like the iterative loop). This phase of the encryption used the Henon map that matched the generated vectors. It is important to note that the Dynamic key generation was essential for the text encryption and generation of certain vectors. In fact, the generated number was limited (from 1 to 26) according to the alphabet characters from A to Z. To take the character from the plaintext, the generated number was executed on the next character associated to the sequence in the alphabetic order. The introduced new order selection algorithm made the encryption process more complex and almost impossible to decrypt. Consequently, the complexity of the generated

key space for the number generator was enhanced. This is performed by inserting a second self-iteration for the control parameters (X) as expressed via the relation:

$$X_{n+1} = 1 - ax_n^2 + bx_{n-1} + y_n \quad (1)$$

Where n is iteration number from 1 to 26, X is the original sequence of the letters, Y is the character position in the cipher text, and a, b are two control parameters (a = 1.4 and b = 0.3) of the dynamic Henon map function. Figure 5 shows an example of proposed encryption process for the word COMPUTER.

The coordinate of C (1,3) in Fig. 5 represents the first order in the text and the third order of letter C in the alphabetic sequence. The second column represents the new generated order and corresponding order in the alphabet can be generated via:

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

Where Y new represents the new second column in Fig. 5.

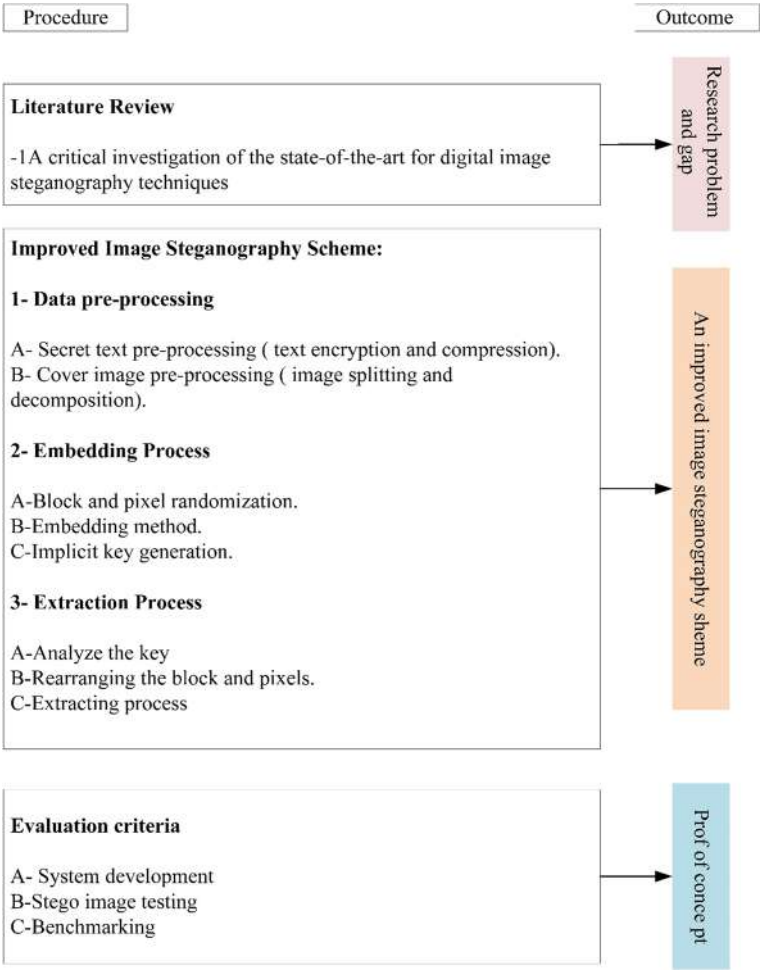

Fig. 4 The general framework of the study

The suggested encryption method first limited the key space and generated random number (between 1 to 10) and then assigned another limit to the second vector (between 1 to 100), and so on. The number generated by the proposed method had variable threshold or limit that was chosen experimentally which was changed later for the second iteration in the loop as depicted in Fig. 6.

More specifically, the generation of the keys during text encryption begun with the random number series based on the Henon map wherein the number of control iterations depended on the text length. The initial point was set to 0.323 that was chosen experimentally. Next, the Henon function generated four random elements considered as the initial for the next three iterations as follows in Table 1:

Later, the logistic map was implemented four times as produced by the four elements series of the Henon map, where each of them was considered as initial value for the next iteration as shown in Table 2.

The initial value is the main feature of the randomness to encrypt the text files. The random process is illustrated in Algorithm 1.

Algorithm 1 Random element selection process

Input: Four (RND) vectors

Output: one (RND) Vector

Begin

{**For** all RND vectors **do**

If Amended Bernoulli > 0.34 **then** select element from Iteration1 vector

If 0.34 = < Amended Bernoulli < 0.67 **then** select element from Iteration 2 vector

Else the selected element is from Iteration 3 vector}

End

The most important criterion for evaluating the text encryption is the histogram because of its ability to illustrate the frequency of letters throughout the text. The redundancy of each character should be near the normal or average of other characters. Thus, through the randomness, the redundancy of the letters was changed especially when the text was segmented into the proper fragments before the encryption process begun. The transfer of the letters during the encryption by the random function was worthy when there was uniform letter redundancy within the text as displayed in Fig. 7.

The whole secret text required to find the method that could depict or illustrate this procedure. Thus, the histogram for the letter within the text was proposed which normally showed the frequency of each item that needed to be measured. For the proposed scheme, the

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

Fig. 5 COMPUTER word encryption process

histogram showed the redundant characters for each segment. Fig. 8 elucidates the frequency of the text in terms of the histogram.

The randomness still needs to be improved because of the normal random functions (Fig. 4.6) must be normalized for rearranging the distribution of the letters inside the text. Two control parameters can enhance the histogram even when the iterations and segmented text are reduced. The aim of the proposed encryption method was to secure the text inside the image. Thus, the final text before embedding was uniform, implying that the difference between the peaks was insignificant. In other words, the frequency of the letters inside the text is approximately equal as shown in Fig. 9.

2.2.3 Enhanced Huffman coding

The main aim of the Huffman coding algorithm is to reduce the size of the text before embedding to the image [50]. The capacity is an important feature of any steganography to make the system more robust in which it is possible to hold a high amount of data inside a hosting image while maintaining the quality of image represented by PSNR. This algorithm is basically based on the frequency of the letters (weight) and text file length or text stream. Thus, the length of the text stream was arranged to make the algorithm sufficient and to get more useful from applying the Huffman algorithm in this system. The proper length or fragment of the text stream made the scheme more reliable and more robust. This fragment procedure is explained below. In the secret message preparation process, the bit stream must be fragmented. After the Huffman coding process, the produced text was converted into the digital form of 0 and 1. The processing of bits stream depended on the length of the data from the embedding stage. These bits were manipulated before embedding to ensure the scheme reliability. In other words, the sample taken from these bits stream was compatible with the process in the embedding stage. Cutting of a given text that represented the bit stream (sample) produced

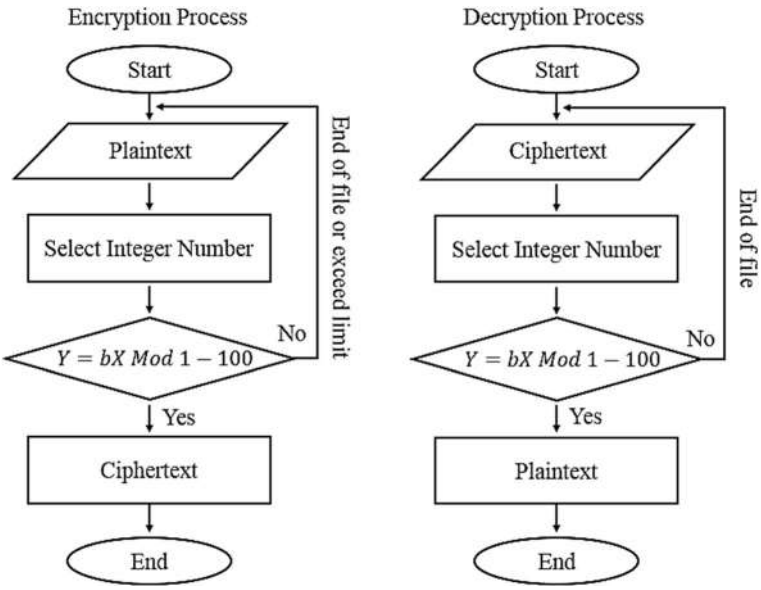

Fig. 6 The encryption and decryption process

Table 2 The initial value and generated next iteration values

0.323	0.977	0.543	0.432
0.219	0.391	0.433	0.675
0.986	0.854	0.942	0.329
0.763	0.657	0.657	0.261

more effects. The data embedding to an image, especially when a down payment of bits is processed as one packet and separated from the original bit stream as illustrated in Fig. 10.

There are many advantages and disadvantages of choosing the long or short fragments. Short ones make the embedding and distribution over pixels easy but lead to low image imperceptibility. Conversely, the long fragments are difficult to embed but at the same time easy to get high PSNR (good imperceptibility). Thus, a compromise was necessary to get the optimum condition. To surmount this shortcoming, the best length was chosen experimentally based on the random equation for 6 iterations that was manipulated separately as a fixed sample. The interval part for separate parts became imaginary as the logic, not physical part.

2.2.4 Cover image pre-processing

Another pre-processing stage is applied to the proposed scheme before the embedding process to achieve an efficient embedding process called cover image preparation. The following sections explain the detailed process of image splitting technique and image transformation decomposition method.

2.2.5 Image splitting technique

This phase covered the selection and analysis of the given image before the implementation of any action on it. In the beginning, an image is selected from the given dataset. Now, if the chosen image is in 8-bit greyscale, then the proposed scheme directly deals with it. However, if the selected image is in 24-bits RGB scale, then the proposed scheme first analyses separately each channel of the RGB image to determine its suitability for the further implementation. After the completion of the separation stage, each image channel in the single 8-bits matrix acquires same dimension as the original image. In short, this stage creates three channels image with each of these channels as an 8-bit image. The idea behind image splitting into three channels is the system must check three values per pixel and find the appropriate one to host the secret bit inside it. Figure 11 depicts the way of analyzing the image channels.

2.2.6 Image transformation decomposition method

To enhance the robustness and effectiveness of the embedding of the secret data, the Fibonacci-based decomposition technique was used [33, 35]. In this work, the decimal number of the pixels was changed directly to the Fibonacci decomposition before applying any process into it. The hidden information inside the cover image considered the Fibonacci decomposition, implying that the data became a part of the image [11]. The bitplane of the cover image was the 8-bitplanes due to the binary representation. Thus, the implementation of the Fibonacci

decomposition transformed it to the 12-bitplanes logically, making it convenient for the embedding process concerning the imperceptibility of the stego image. The difference between (binary representation) the 8-bitplane and (Fibonacci representation) 12-bitplane in the embedding process was substantial because, the LSB in the 12-bitplane embedment was more efficient and robust than the 8-bitplane, the reason is due to the bitplane (1) of the Fibonacci decomposition is darker than the bitplane (1) of the binary decomposition. This means that intruders cant observe the patterns (hidden bits) in the bitplane(1), and this in turn gives higher robustness for the proposed study. In order to explain the method of analysis of any pixel value from the decimal to Fibonacci representation using the Fibonacci sequence, the Zeckendorf's theorem was applied on this sequence in which the general formula of the Fibonacci sequence produced [54]:

$$F_1 = 1, F_2 = 1, F_3 = 1 + 1 = 2, F_4 = 2 + 1 = 3, F_5 = 3 + 2 = 5\ldots, F_n = F_n{-}1 + F_n{-}2$$

In general, the Fibonacci theory can be summarized as:

$$F(n) = \begin{cases} 0 & if\ n = 0 \\ 1 & if\ n = 1 \\ F(n{-}1) + F(n{-}2)\ if\ n > 1 \end{cases} \tag{3}$$

Generally, each number in the Fibonacci sequence of numbers is the sum of the previous two numbers. The Fibonacci sequence begins not with 0, 1, 1, 2 as the modern mathematicians do but with 1, 1, 2, etc. The calculation is carried to the thirteenth place (fourteenth in modern counting) that is 233, though another manuscript carried it to the next place that is 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377. The Fibonacci did not acknowledge about the golden ratio because the limit of the ratio of the consecutive numbers is in this sequence. Algorithm 4.3 shows the steps for achieving the Fibonacci number sequence.

Algorithm 3 Fibonacci number

Input: An integer n for n-th Fibonacci number.

Output: n-th Fibonacci number.

```
    FN[0]←0
    FN[1]←1
for i←2 to n-1 do
    {
        FN[i]←FN[i-1]+FN[i-2];
        i=i+1
    }
Return FN[n-1]
```

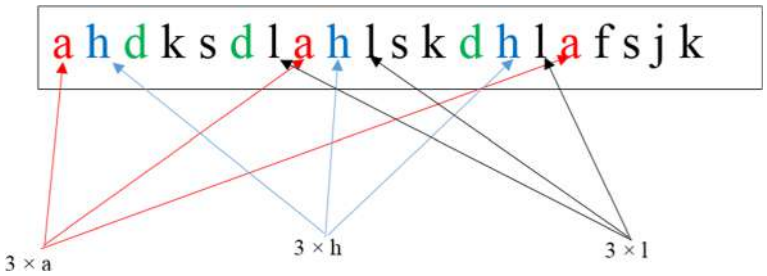

Fig. 7 The ideal encryption result when a frequent letter is equal for most letters

The Fibonacci decomposition was used mainly for three important reasons:

i) The change to the Fibonacci decomposition enabled to improve the security due to difficulty of estimating the secret data by the attacker.
ii) It increased the robustness of the system because of the use of 12 bit-planes.
iii) It was difficult to recognize by the visual attack because of the heterogeneous data.

In the present study, the Fibonacci was a logical sequence used to illustrate the decimal number of the pixel value consisting of the summation of two previous numbers used here for increasing the robustness of the system. Using the Fibonacci decomposition, the proposed scheme together with the DGV became more secure and robust. Basically, the Fibonacci was the summation of the previous two numbers in the sequence except the first and second numbers as depicted in the simple algorithm hereunder:

```
public int Fibonacci (int x) {
        if (x==1) {
                        return 1; }
        else if (x==2) {
                                return 1; }
                else {
                        return Fibonacci(x-1) + Fibonacci(x-2) }
                        }.
```

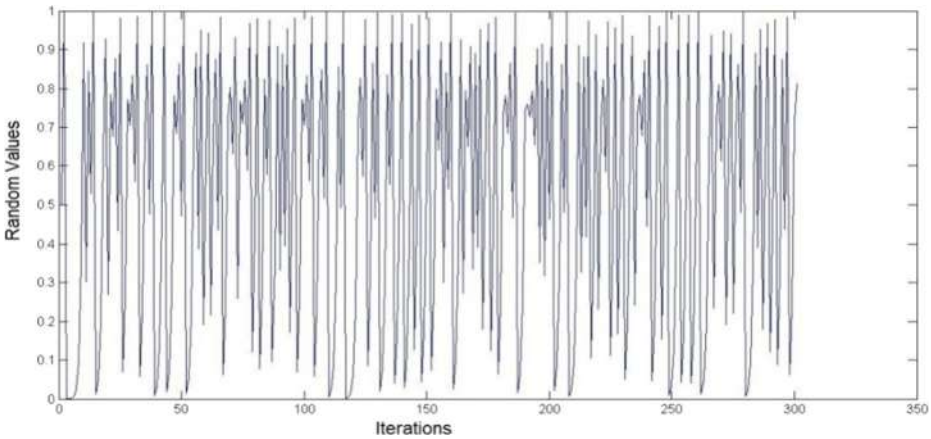

Fig. 8 The histogram of the text when one random was applied for many iterations

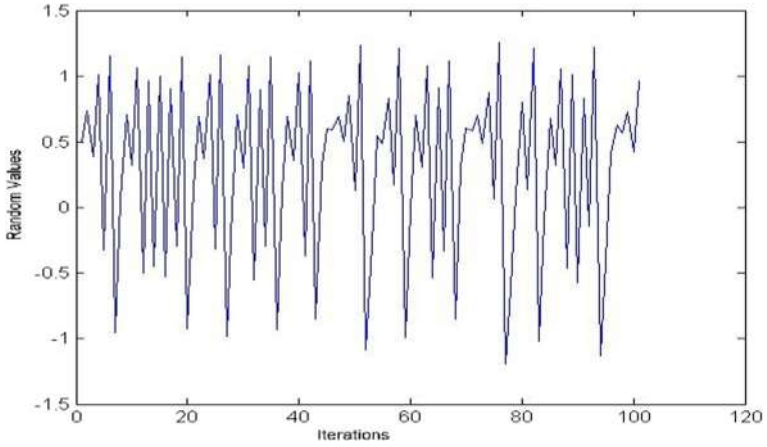

Fig. 9 The normalization of a histogram for the secret text

2.3 The proposed embedding method

The basic essence of the proposed steganography scheme is to hide the secret message in the certain image (original image) and keep the quality of the hosted image as identical as the original image and transfer it from the sender to the authorized receiver side without causing any doubt to the unauthorized users even in the presence of some text inside it. This study proposed a new steganography method to hide the secret message inside the cover image using three main stages to get the secure stego-image such as random blocks and pixels selection, contrast level condition, and implicit key generation. The lack of awareness of the intruder regarding the existence of some text inside the image is the main aim of the proposed robust image steganography system development. The following subsections describe the three stages of the proposed embedding method called the Distinction Grade Value (DGV).

2.3.1 Random blocks and pixels selection

The primary advantage of developing an ISSs is to provide a secure environment in which to secret messages within the stego-image can carry the sensitive data information over the WWW. As the initial stage, the image was divided into 8×8 blocks each with 64×64 pixels. First, the block was selected then from this block the pixels were chosen for the embedding purpose as shown in Fig. 12, where the partitioning of the 262.144 pixels (512×512) were performed. The random

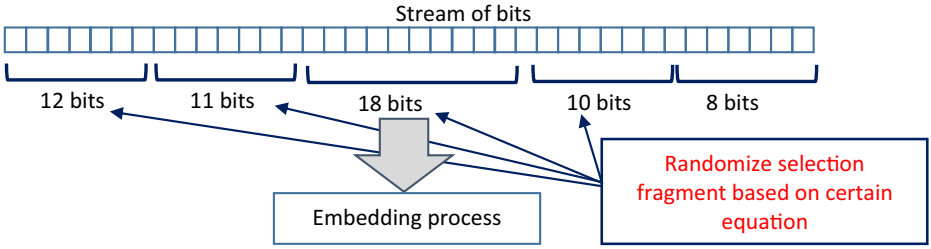

Fig. 10 The bit stream fragmentation using the proposed method

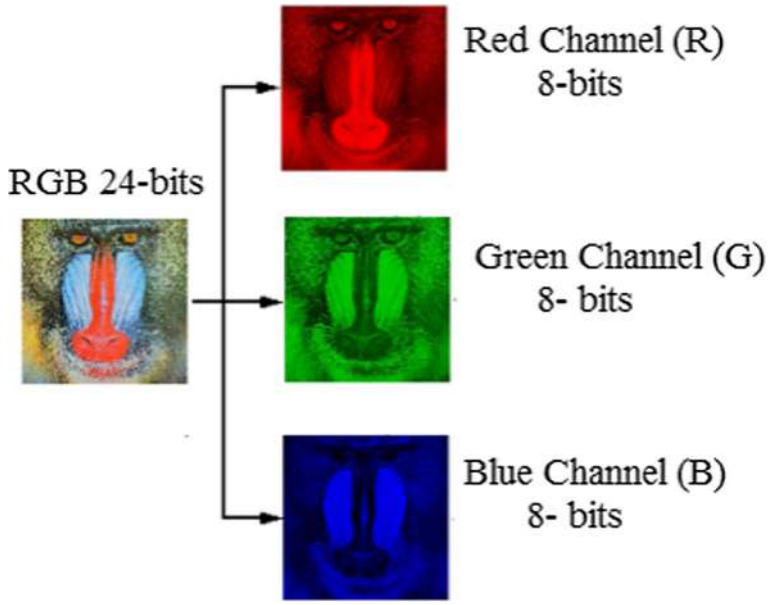

Fig. 11 Image analysis into RGB channels

process is responsible for dividing the cover image into sub-blocks, where three rounds of the random function were used in this process to select the use of the first pixel for the embedding. Normally, the steganography system uses either round random function or other algorithm like Knight Tour or one control parameters (Henon map) for the random process. For the high security issues regarding the proposed scheme, two control parameters were used in the Henon random function. This random function is beneficial in term of increasing the complexity of the aimed blocks or pixels selection processes up to 10^{30} round steps (theoretically). Actually, for achieving the high security, a random function is used. The number of attempts in the Henon map function was 10^{30} that produced around 2^{100} random process which is enough to secure the text inside the image. The normal random function used a single parameter to choose the number, where the initial condition for this function (single) is 10^{15} random processes and probability of finding these numbers are 2^{20} random processes two control parameters are used as a constant number in the equation to increase the complexity of the numbers estimation.

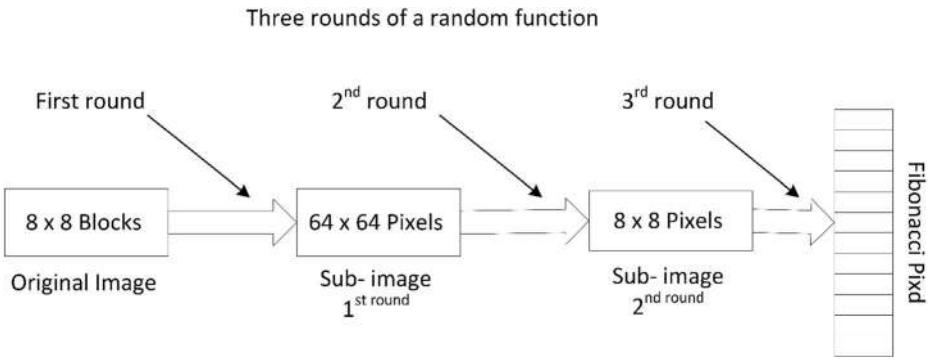

Fig. 12 The process of dividing a cover image into blocks

Consider the number x of the cover image blocks. Then, the image can be dividing into k = 64 blocks (that is changed after first random rounding) to create the vector of size x. Since, every p is involved in the domain of b_i such as $p = x/k$ and thus is an integer value.

$$b_i = i + \left(\mathrm{k}^* p\right) \tag{4}$$

$$vector = [b_1 b_2 b_3 b_4 \ldots . b_k] \tag{5}$$

where b_i is the i^{th}block and the *vector* represents the place to store labeled blocks. Keeping track of the randomized blocks was necessary because of its requirement in the embedding stage and to reveal the secret message via a stego key. Figure 13, shows the steps to achive the randomized blocks.

2.3.2 Distinction grade value method (DGV)

The purpose of applying the proposed DGV method is to achieve improved security of the steganography scheme. Each pixel in a colour or grayscale image consisted of decimal

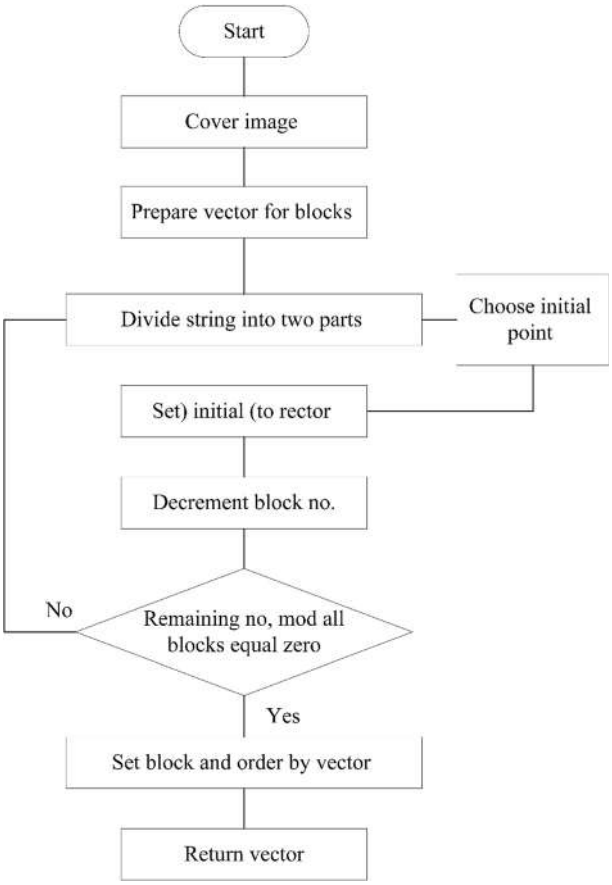

Fig. 13 The randomized blocks in the random stage

numbers that represented the contrast of this pixel or illumination. The grey image is comprised of one decimal value from 0 to 255 (represented in the binary 2^8 occupy 8 bits) where the zero value reflects black pixel while 255 value reflect white pixel and the grayscale starts from the white and ends in black. Most of the differences between the contrasts are at the edges and boundaries of the object, especially when moved from the low to high contrast or vice versa. Figure 14, shows the contrast area with the corresponding decimal representation. Figure 14(a) clearly displays different contrast and crossover from the low contrast at the upper left corner to the high contrast at the bottom right corner. The sharp diagonal edge located in the same (Fig. 14(b)) contrast when moved between two adjacent pixels with different large values. Due to the little variation between each pair, the best location to embed the secret message is shown in Fig. 14(d). Human eye can recognize the difference in the contrast around 30 pixel values. However, insertion in such area often differs as the maximum of two pixel values.

The colour image is consisted of three values for each pixel such as the Red, Green, and Blue (RGB). These pixels are represented by 24-bits (3 bytes) with one byte for each colour channel. The embedment in such area is more flexible because of the ability to jump over these three bytes. Therefore, the embedment in the colour image is more complex than grey image because three channels need to be checked by comparing three pixel values. When the condition for the pixel embedment is satisfied, then the system is ready for covering the secret bit. Figure 15, illustrates colour images with the corresponding pixel values.

To vary the contrast in the colour image, one must check three values per pixel and find the appropriate one to host the secret key. Often, the varying contrast is located in three channels and positioning a fraction of it in one channel is not easy that need to pass many conditions. Critical condition leads to the robust embedding method that takes care of the condition and thresholding becomes essential. As aforementioned, any embedding method consists of two processes such as the pixel selection and data insertion processes. The pixel selection is responsible for achieving the enhanced security and imperceptibility of the data hiding system.

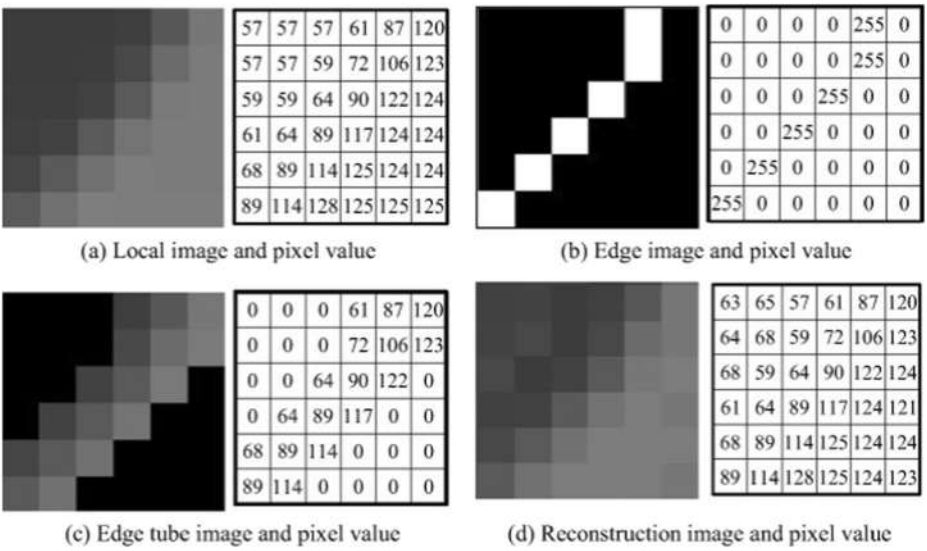

Fig. 14 Location of the contrast value with the corresponding pixel value

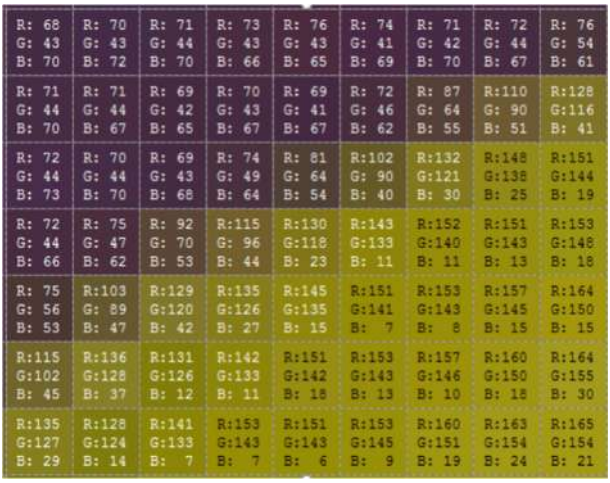

Fig. 15 Colour image representations in terms of pixel values

In this perception, present study aimed to maintain these two criteria. The pixel selection is accomplished in two stages. First stage is the movement around the image via single movement strategy. Second stage checked the condition for embedding. These two stages actually operated simultaneously and one completed the other. The selected pixels are accumulated in one vector. Upon completing the selection process, these pixels were randomly rearranged according to the new random technique while keeping the index for each pixel. The 8 neighbour's strategy is used to move over the image according to one condition related with contrast value. These 8 neighbours covered the image and moving vertically, horizontally, and diagonally as illustrated in Fig. 16.

Certain pixels are considered as the coordinate position in the image matrix where such pixel could move in every direction by increasing or decreasing the x-axes and y-axes. The proposed scheme compared the values of the centre pixel (x,y) and its neighbours (±x, ±y). When these pixel values differed according to the threshold, then the position of this pixel is

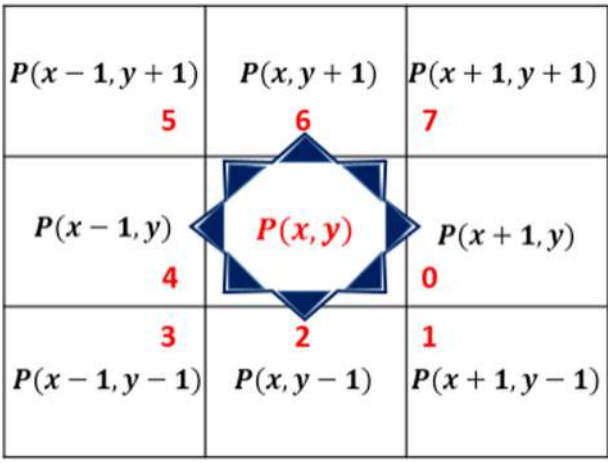

Fig. 16 The 8 neighbours' pixel movement strateg

saved in the vector form and moved accordingly. Otherwise, it was skipped to the other pixel coordinate. Consequently, the pixel is positioned in the middle of two areas of high and low contrast; wherein the embedment of the secret bit was in the side of near brightness. For example, when the difference between two pixels' value is according to the threshold chosen experimentally (such as the 4 decimal value) then the secret bit is embedded in two pixels beside the certain pixel. Conversely, when the secret bit was 0, then the secret bit is either embedded with the high value or else (secret bit 1) with the low contrast value and so on as explained in Fig. 17. The contrast level check of each pixel enabled to scan the entire image for choosing the suitable location (pixel) to hide the secret bit. Subsequently, this method produced high imperceptibility and high security, indicating the success of the proposed steganography scheme. In addition to the pixel selection strategy the pixel replacement must be applied to further enhance the imperceptibility and security of the data hiding algorithm which is discussed below.

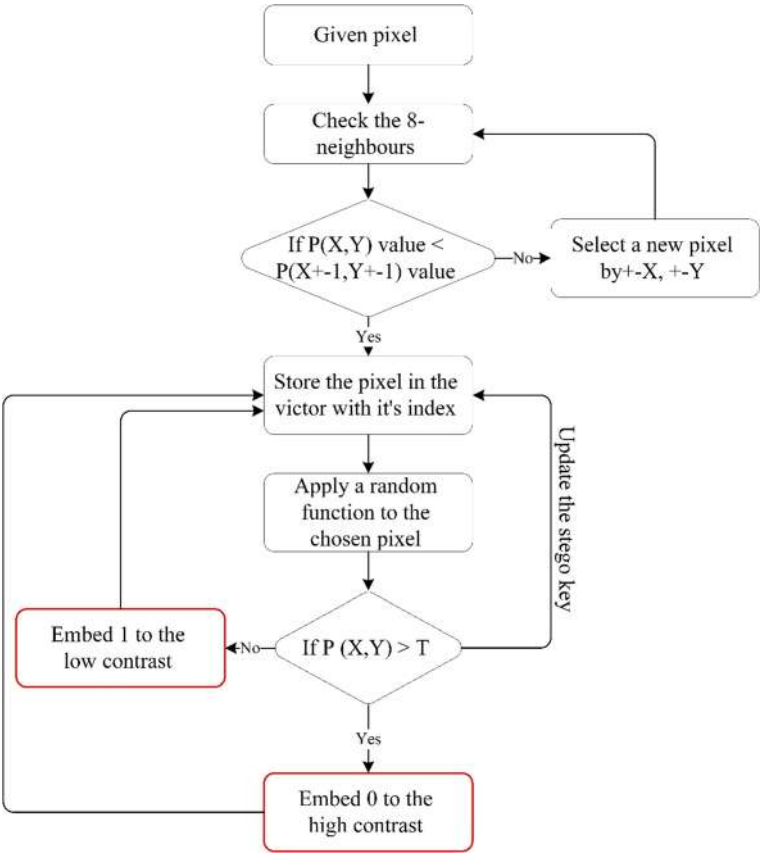

Fig. 17 The proposed embedding strategy

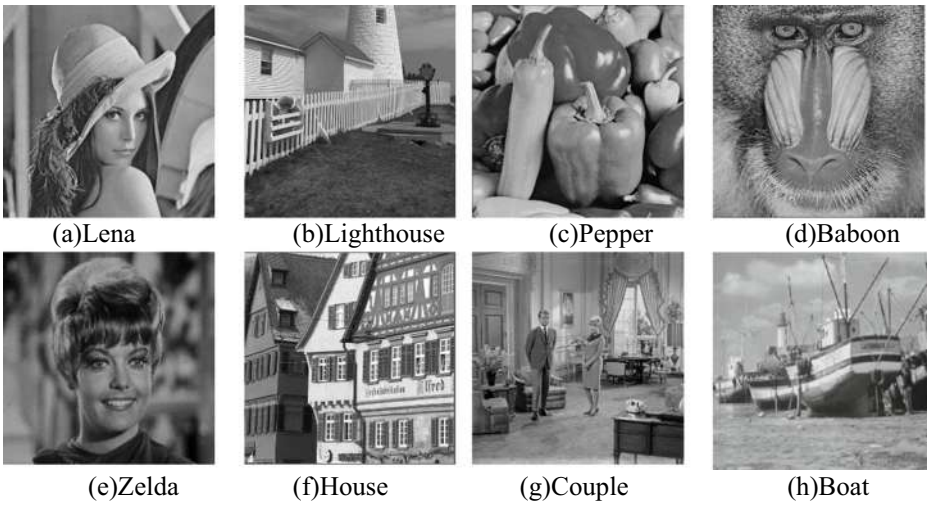

Fig. 18 (a-h) Stego images for the proposed ISS obtained with the EP of 12.5%

3 Result and discussion

The applied processing via the proposed scheme that affected the image quality and led to some information loss is ascertained through various evaluation measures. The evaluation procedures of the stego image can be objective and subjective. The objective methods depended on finding the differences by applying the numeric criteria and using several criteria such as ground truth or prior knowledge of statistical issue. Conversely, the subjective methods depended on the observation of humans and judgment without any referred criteria. The present study considered the standard evaluation measures (objective methods) to validate the proposed scheme including the embedding capacity (EC), peak signal to noise ratio (PSNR), mean square error (MSE), bit per pixels (BPP), structural similarity index (SSIM) and normalized cross-correlation (NCC). The EC value can be defined as ratio of the number of message bits to the number of cover pixels [21] which is directly related with the number of pixels used in the proposed scheme. Different number of message bits were embedded by one pixel and the EC is expressed as:

$$EC = \frac{\text{The number of message bits}}{\text{The number of cover images's pixels}} \tag{6}$$

The following parameters are used in the simulation:

Table 3 The values of PSNR for the **gray scale Baboon** image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)		
	Simple LSB	Fibonacci	Proposed Scheme
6.25%	65.722	69.221	77.417
12.5%	59.932	63.119	71.928
18.75%	58.110	62.883	70.277

Table 4 The values of PSNR for the **gray scale Lina** image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)		
	Simple LSB	Fibonacci	Proposed Scheme
6.25%	61.921	65.338	73.009
12.5%	52.182	63.976	72.142
18.75%	49.992	61.196	69.677

i) For a given image of dimension (512×512) pixels, 16,384 bytes corresponded to 6.25%, meaning that every two pixels represented 16 bits, thus 1/16 = 6.25% when 1 bit of two pixels was embedded.
ii) For a given image of dimension (512×512) pixels, 32,768 bytes were equal to 12.5%, implying that every pixel corresponded to 8 bits, so that 1/8 = 12.5% when 1 bit of one pixel was embedded.
iii) For a given image of dimension (512×512) pixels, 49,152 bytes corresponded to 18.75%, signifying that every two pixels were assigned to 16 bits, accordingly 3/16 = 18.75% when 1.5 bit of one pixel was embedded.

In the current study, diverse payload capacities were used and presented as the percentages in order to be consistent with that reported literatures in this field. Figure 18(a-h) shows different stego images used in the proposed ISS with embedding payload (EP) of 12.5%.

To evaluate the image quality, PSNR is calculated after the embedding process and a comparison was made between the original and stego images. The process of data embedding is considered to be imperceptible to the HVS when the result of the PSNR is ≥30 db [13]. The value of PSNR is calculated using the expression:

$$PSNR = 10.log_{10}\left(\frac{255^2}{MSE}\right) \tag{7}$$

with

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \tag{8}$$

where MAX is the maximum possible pixel value of the image; m and n are the dimensions of the image; I and K are the corresponding original and noisy pixel.

The PSNR value is based on the MSE that affected adversely. The parameters of PSNR allowed normalizing the equation for all methods and image types. During the implementation

Table 5 The values of PSNR for the **gray scale Tiffany** image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)		
	Simple LSB	Fibonacci	Proposed Scheme
6.25%	60.001	64.141	72.806
12.5%	58.919	62.770	71.983
18.75%	57.001	60.899	69.866

Cover image Simple LSB Fibonacci LSB Proposed DGV

Fig. 19 Lina stego image using three different methods with the EP 18.75%

of the proposed ISS two important stages are involved namely the training and testing. In the conventional image processing, the imperceptibility of the stego image is determined using the PSNR measures [31]. By applying the PSNR measures, the fidelity of the stego image can be evaluated against the original carrier image. In other words, the level of distortion in the stego image can be measured against the carrier image in the units of decibel (dB). A higher score of the PSNR corresponds to the high quality image, thereby minimizes the detection probability of the attack using the HVS [41]. Using the training phase, the PSNR became less when the MSE is large, implying that the mismatching is increased between the original image and stego message. For high MSE, the result is not satisfactory in terms of the PSNR because of their inverse relationship. This problem is overcome in the testing stage and the achieved results are better than the one obtained by others.

The BPP yields the average number of bits that can be hidden per pixel [21], whereas the FOBP is the number of pixels that exceed the permissible range of 0 to 255 after the secret data is embedded. Thus, to measure the similarity between the original image and the stego image the value of SSIM was used [22]. The value of SSIM (ranged from - 1 to 1, wherein 1 indicated no difference between the original image and stego image) was calculated via:

$$SSIM = \frac{(2P_O\, Q_S + C_1)(2\sigma_{OS} + C_2)}{\left(P_O^2\, Q_S^2 + C_1\right)\left(\sigma_O^2 + \sigma_S^2 + C_2\right)} \tag{9}$$

where P_O, P_O^2 and σ_O^2 corresponding to the original image as well as Q_S, Q_S^2 and σ_S^2 for the the stego image denote the respective mean pixel value, variance and standard deviation. The covariance between the original image and stego image is represented by σ_{OS}. $C_1 = k_1 L$ and $C_2 = k_2 L$ are constants with $k_1 = 0.01$, $k_2 = 0.03$, and $L = 255$ for the grayscale image.

In the present work, three types of embedding were used to evaluate the performance of developed ISS with different EP, simple LSB embedding, embedding with Fibonacci

Cover image Simple LSB Fibonacci LSB Proposed DGV

Fig. 20 Tiffany stego image using three different methods with the EP 18.75%

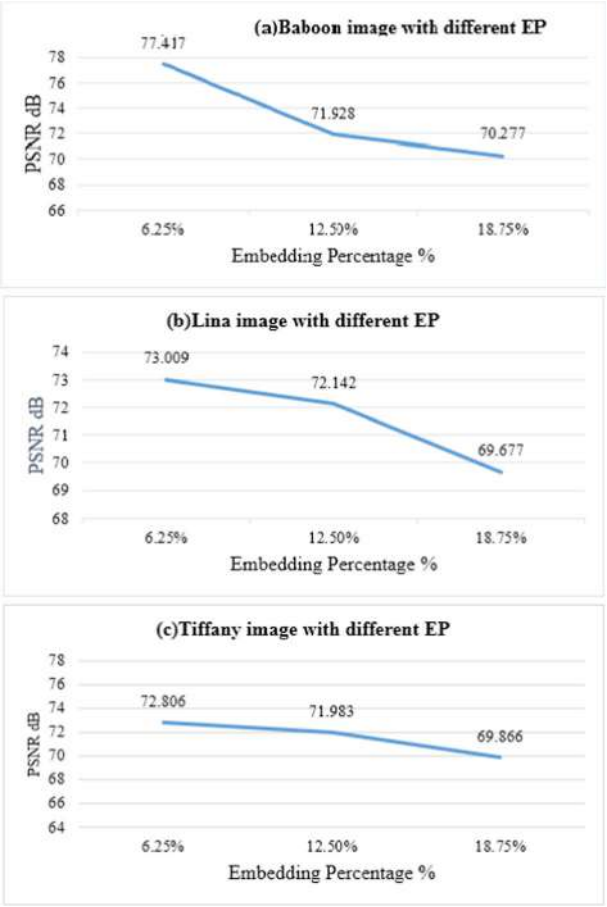

Fig. 21 The PSNR outcomes of the proposed DGV method for the grayscale images (a)Baboon, (b)Lina and (c)Tiffany with different EP values

decomposition and embedding using the proposed DGV method for the gray scale standard SIPI images (Lena, Baboon and Tiffany (512×512)). The obtained results are presented in Table 3, 4 and 5.

The results clearly revealed that the Fibonacci decomposition produced better PSNR than the simple LSB. This is because the PSNR factor took the frequency of bits in the LSB of the cover image and the Fibonacci decomposition had less effect on the binary cover image.

Table 6 The values of PSNR for the color Baboon image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)		
	Simple LSB	Fibonacci	Proposed Scheme
6.25%	59.910	63.811	70.080
12.5%	57.919	61.001	68.402
18.75%	55.999	60.128	67.849

Table 7 The values of PSNR for the color Lena image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)		
	Simple LSB	Fibonacci	Proposed Scheme
6.25%	57.001	60.909	67.425
12.5%	54.998	57.890	65.520
18.75%	54.888	57.148	64.211

Moreover, the embedment of the secret message is performed after converting the pixel into the Fibonacci decomposition and storing the pixel in the binary form of the stego image. Thus, the reflectance is less than that of the simple LSB. The proposed DGV method is useful due to the integration of the Fibonacci decomposition with tools of the secret preparation (new SSSM algorithm and enhanced Huffman coding). In addition, the redundant pixel values with many frequencies made the bits inside the image more chaotic, thereby increasing the PSNR values. It is worth noting that the PSNR always checks the uniformity of the pixels inside the image.

As mentioned earlier, the imperceptibility in the ISS indicates that the embedded secret message must not be detected by the human eyes. Two significant factors could affect the imperceptibility of the stego image. First, the embedding of the little data into the image could increase the imperceptibility of the payload capacity. Second, the embedding method itself could affect the normalization of the bits in the LSB image. It can be concluded that the imperceptibility was synonymous with the PSNR in the proposed ISS. Thus, the two methods are used to evaluate the imperceptibility such as the PSNR and HVS attack that is based on the human eye to judge.

The main objective of the ISS is the secret message when embedded into the image will become unseen or invisible to the human eyes. Only the sender or receiver can know using the special procedures. With all the methods, the image must not be recognizable but the difference gives the ability to withstand the attack. Thus, the imperceptibility of the proposed ISS is very important as it reflected how the secret message was maintained inside the image as exemplified in Figs. 19, 20 and 21.

Similar results are revealed that for the human eyes in all three different methods (LSB, Fibonacci LSB and proposed DGV method). The Baboon image appeared the same after embedding (16,384, 32,768 and 49,152 bytes), but actually each had different PSNR. However, the insertion amount of the payload is limited and after this limit, the image was distorted and became visible to the human eyes. These results are obtained for the gray image dataset. The same procedures are followed for the colour image using the proposed ISS. The difference between the gray and color images was only in the representation of the pixels.

Table 8 The values of PSNR for the **color Tiffany** image obtained using three types of embedding with different EP

Embedding %	PSNR (dB)		
	Simple LSB	Fibonacci	Proposed Scheme
6.25%	57.999	62.644	69.276
12.5%	56.998	60.127	67.464
18.75%	54.339	57.917	65.909

In the gray image each pixel was represented by 8-bits while in the colour image each pixel had 24-bits made up of 8-bits for the Red, 8-bits for the Green, and 8-bits for the Blue. In this case, the presence of three LSBs is responsible for holding the secret data. Figure 21(a, b and c) shows the results for gray scale Baboon, Lena, and Tiffany (512×512) images with different payload capacity. These three images are selected from the widely used and referred SIPI dataset that made the benchmarking easy.

The results for the gray scale images clearly showed that the proposed scheme can handle the color images taken from the same standared dataset. Tables 6, 7 and 8 illustrates the obtained PSNR values for the three types of embedding (simple LSB, Fibonacci decomposition and DGV) used to evaluate the performance of the proposed ISS with different EP for colour standard SIPI images (Lena, Baboon and Tiffany (512×512)).

Generally, the calculated PSNR values for the color images are lower than the gray scale images due to the representation of color pixels image with 24-bits for one pixel as opposed to only 8-bits for the gray scale. Figure 22(a, b and c) depicts graphically different results for the

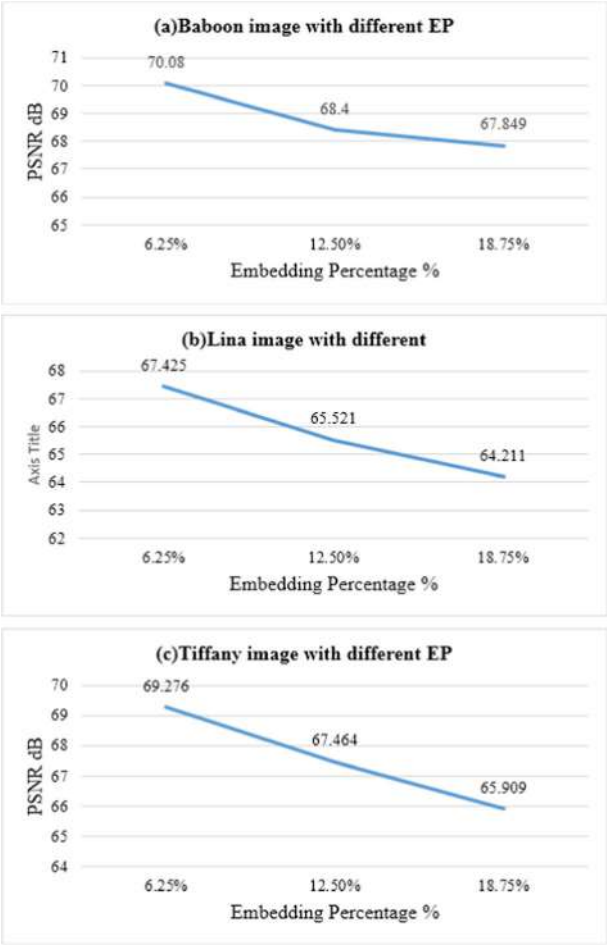

Fig. 22 The PSNR outcomes of the proposed DGV method for the colour images (a)Baboon, (b)Lina and (c)Tiffany with different EP values

imperceptibility obatined using the colour Baboon, Lena, and Tiffany (512×512) images with different payload capacity.

The PSNR values for the colour images are different from the gray scale images, indicating different imperceptibility. In addition, the Baboon image showed a higher PSNR value which is due to the different properties of this image and also the nature of the image itself that has more contrasts in the pixels value, thereby enabling the Baboon image more chaotic. Additionally, the DGV method being dependent on the value of the pixel's contrast, the Baboon image produced higher PSNR than the other images accompanied by a wide soft area (less contrast).

The primary goal of the proposed ISS is to keep the stego image same as the original image as viewed by the naked human eye or via the statistical methods when using a limited payload capacity. In the proposed method used different evaluation tools like PSNR, MSE, SSIM, NCC, and FOBP to check the stego image before sending it to the authorized receiver to ensure that familiar attacks like HVS, Chi-square and Histogram are unable to detect the secret message. Figure 23, shows the similarities between the stego images and the original image with different Paylaod capacity.

The original image appeared like a stego image with an acceptable amount of embedding such as the second row of the figure. However, when it exceeded the embedding limit the image is destroyed and is detectable to the hacker easily as indicated by the last row in the figure. The efficiency and quality of the proposed scheme is tested on diverse stego images with different amount of EP. Table 9 shows the various evaluation tools with different amount of EP for the standard gray scale (Lina, Baboon and Tiffany (512×512)) images. While,

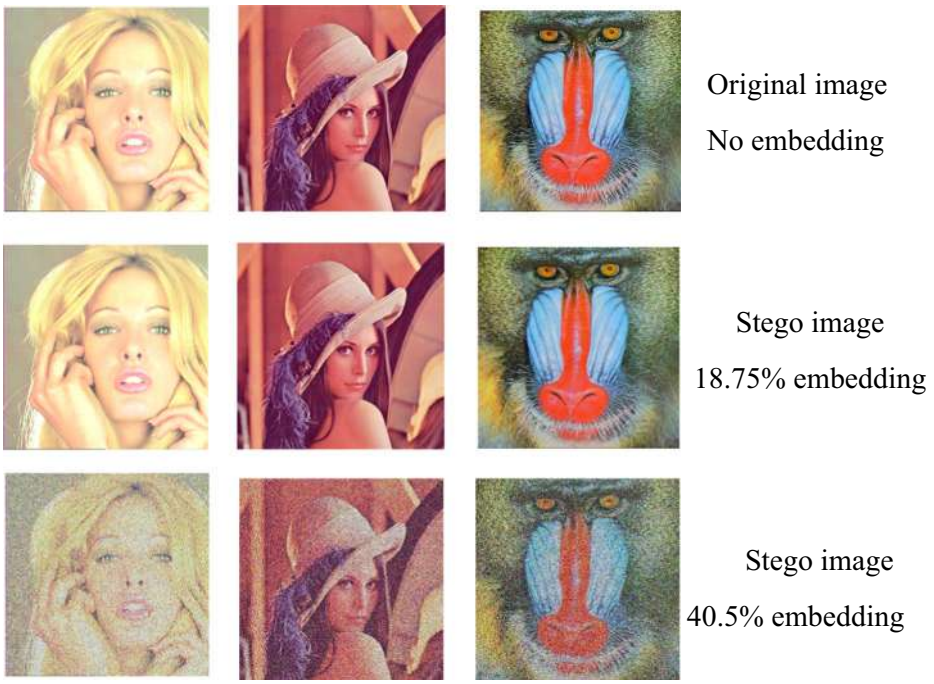

Fig. 23 The stego and original images' resemblance with different paylaod capacity

Table 9 Different evaluation tools with different amount of EP for gray scale images

Image	6.25%			12.5%			18.75%		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
Lina	0.0101	1	1	0.0122	1	1	0.0178	0.9999	0.9999
	6.12%			12.5%			18.75%		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
Baboon	0.0121	1	1	0.0135	1	0.9999	0.0189	0.9999	0.9999
	6.12%			12.5%			18.75%		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
Tiffany	0.0124	1	1	0.0176	1	0.9999	0.0192	0.9999	0.9998

Table 10 displays the results for the standard colour (Lina, Baboon and Tiffany (512×512)) images.

The results obtained using the proposed ISS were compared with the exisiting state of the art techniques (Table 11 and Fig. 24). The evaluation results of the proposed method were found to be better than those reported in the literatures. This indicated that the tools used for the pre-processing and embedding stages in the proposed ISS allowed to improve the results.

Based on the outstanding experimental results obtained using the proposed ISS when compared with the existing state of the art methods, an inverse relationship between the PSNR

Table. 10 Different evaluation tools with different amount of EP for colour images

Image	6.25%			12.5%			18.75%		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
Lina	0.0155	1	1	0.0175	1	1	0.0188	0.9999	0.9999
	6.12%			12.5%			18.75%		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
Baboon	0.0160	1	1	0.0172	0.9999	1	0.0198	0.9998	0.9999
	6.12%			12.5%			18.75%		
	MSE	SSIM	NCC	MSE	SSIM	NCC	MSE	SSIM	NCC
Tiffany	0.0152	1	1	0.0176	1	0.9999	0.0210	0.9999	0.9998

Table 11 Result comparison between the proposed scheme and the state of art for the Baboon color image

Reference / Code	Image/Dataset	EP %	PSNR (dB)	SSIM	BER	NCC	MSE
[33] / **(A16)**	USC-SIPI 512×512	6.25%	46	0.899	0.0217	0.8928	0.0267
[1] / **(B16)**	USC-SIPI 512×512	6.25%	65.9	0.996	0.0151	1	0.0127
[11] / **(C17)**	USC-SIPI 512×512	6.25%	54.5	0.978	0.0183	0.9897	0.0112
[54]/ (D18)	USC-SIPI 512×512	6.25%	50.21	0.957	0.0199	0.8998	0.0240
[46] / **(E19)**	USC-SIPI 512×512	6.25%	51.22	0.968	0.0195	0.8999	0.0236
[22] / **(F20)**	USC-SIPI 512×512	6.25%	58.22	0.981	0.0171	0.9994	0.0122
Proposed Study / (P20)	USC-SIPI 512×512	6.25%	70.08	1	0.0140	1	0.0101

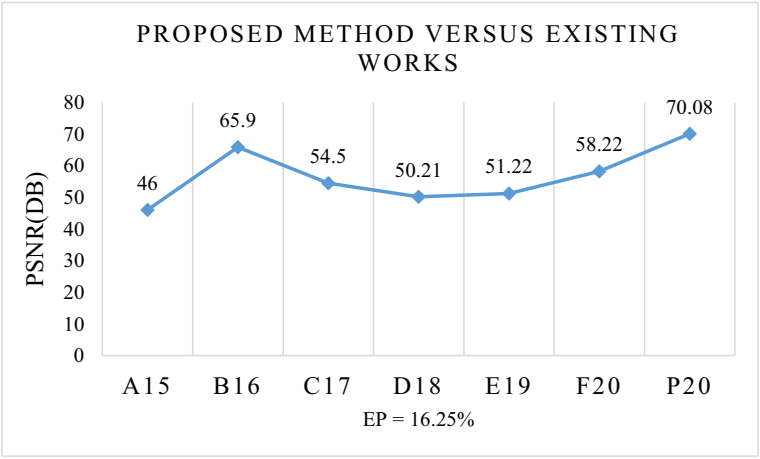

Fig. 24 Comparison study of DGV method versus the existing state of the art methods

and EP is established. An increase in the EP value led to distort the image visual quality and thus reduced the percentage of the PSNR. It is asserted that all the existing methods maintained the balance between the capacity and PSNR by developing an embedding method or improving the secret data before embedding [5, 34, 47].

Based on the findings, it is concluded that more than 80,000 bytes embedment can distort the image and make it visible to the human eye. This further indicated that the image had less imperceptibility. Thus, embedment of 16,000–30,000 bytes can be more reasonable because of the high PSNR values that are unnoticeable to many attacks. It is affirmed that an increase in the payload can cause a reduction in the PSNR values and vice versa.

4 Security evaluation

The present study discussed several structural and non-structural attacks, and the Stego image is tested prior to sending to the receiving party by attacking the stego image with various attacks such as Chi-square, Histogram, and HVS. The main goal of attacking the Stego image

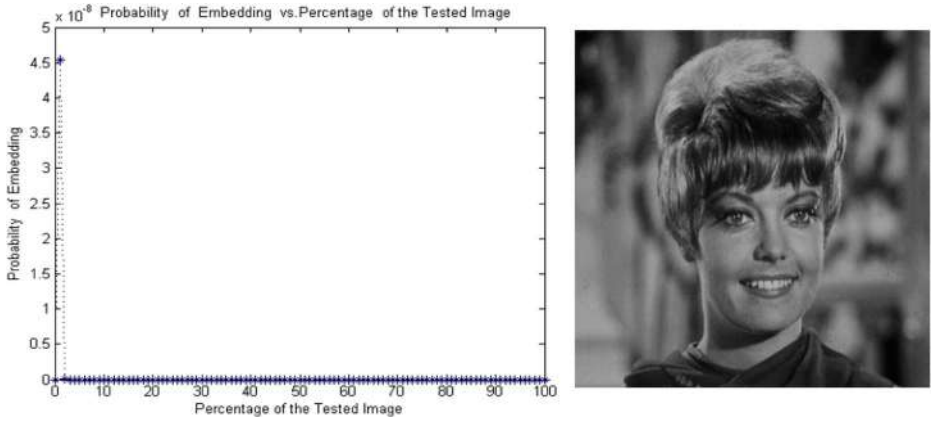

Fig. 25 The χ^2-test for the proposed method after embedding 16,384 bytes for Zelda gray-scale image

with these attacks is to discover the robustness of the proposed scheme. The current section presents the results of the proposed scheme through the three mentioned attacks.

During the embedding process, the secret bit gets located in the LSB bits of the pixel. Thus, the first bit plane faces the degree of change according to its condition. During embedding, the

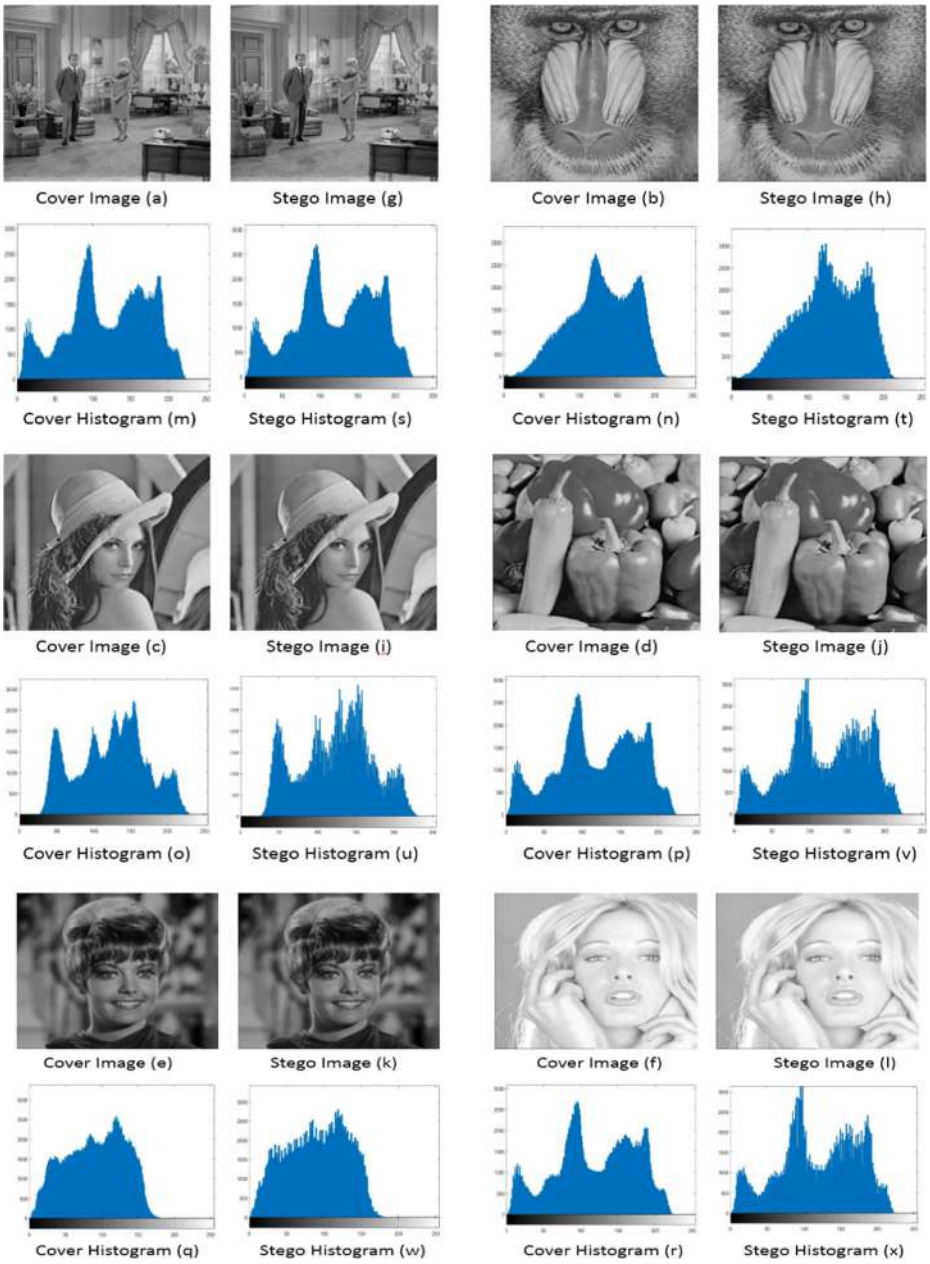

Fig. 26 Comparison of histograms analysis for standard images. The figures are (a) Couple, (b)Baboon, (c)Lina, (d)Pepper, (e)Zelda and (e)Tiffany

systematic changes that occur in the first bit plane can be recognized by the human eye after analyzing the image. However, there is a special attack called Chi-square (χ^2) that is based on the statistical analysis of the Pairs of Values (PoVs) exchanged during the secret data embedding which is also based on the probabilities distribution. The χ^2 attack can find the probability of embedding the secret bits inside the stego image where the normal image follows the usual behaviour. However, due to embedding this behaviour changes and it becomes easy to estimate the order. The χ^2-statistical attack shows the probability of embedding the hidden data in the image by checking the frequency of the LSB in the stego image. Figure 25, shows the χ^2 test for the Stego image with 16,384 embedding bytes for Zelda gray-scale image.

While, the histogram analysis is generated from the embedding process using a group of gray scale images like Zelda, Lena, Couple, Pepper, Baboon and Tiffany as shown in Fig. 26. Generally, by embedding the secret bits in the cover image, the frequency of pixels' values is changed and can become visible (noticeable) in the histogram analysis. Figure 26(m, n, o, p, q and r) shows the frequency histogram of the cover images (original images). Meanwhile, Fig. 26(s, t, u, v, w and x) shows the frequency histogram of the stego images (image before embedding). As shown in histograms analysis, the variance between the constructed

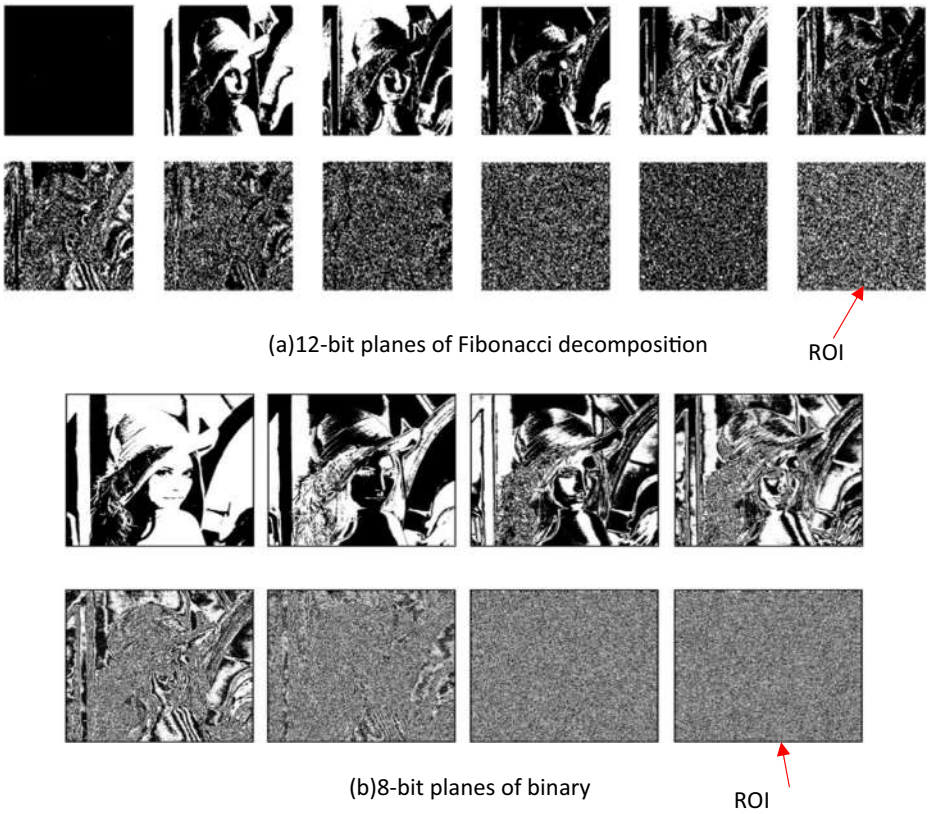

Fig. 27 The difference of distinction between the (a)Fibonacci and (b)binary bit plane decomposition with the region of interest (ROI)

histograms is comparatively less for all tested images. The results appear that distortions generated from the embedding process are unnoticeable to human visual perception.

Finally, the use of 12 bits in embedding can confuse any statistical attacks wherein the up-normal distribution of the pixels in the Fibonacci structure also enhances the robustness of the steganography scheme. The use of Fibonacci in the LSB embedding is less effective for the pixel value than binary the decomposition because it keeps the imperceptibility and robustness as high as possible. Therefore, the 12-bit planes can represent the stego image while the binary image uses 8-bit planes. In the present study, the bit plane is also used to check the image and its quality where it reflected the degree of the image embedment into the first two-bit planes. Figure 27(a and b) presents the distinction between the Fibonacci and binary bit plane decomposition with the region of interest (ROI).

5 Conclusion

In this study, a robust image steganographic scheme for the secure transmission of secret data over the internet is proposed. A steganographic method that focuses only on image visual quality or payload is not efficient to be used in present security applications. This study presented the experimental results, analyses, discussion and comparison obtained from the proposed steganography scheme. Three main criteria are presented to evaluate the finding where it addressed the most important issues in the steganography scheme. These include the capacity and robustness enhancement using a new decomposition technique that is not familiar to the hacker. The system security is improved via the introduction of the new embedding method that is based on the distinction grade value and integrity system of using encryption and random selection during the embedding process. In addition, for each criterion, the results are presented in the tabular and graphical form for the easy interpretations and understanding. This work opened up several new avenues that are worth doing for the future. For instance, the security can be enhanced by mixing the frequency domain and the special domain. This may achieve better results in terms of security and robustness. In addition, the proposed method can be combined with the DWT and embedding may results in high coefficients based on the obtained findings. Many methods have already used high coefficients for the embedding. However, the use of DGV may yield better results in terms of security and imperceptibility.

References

1. Abd El-Latif AA, Abd-El-Atty B, Hossain MS, Rahman MA, Alamri A, Gupta BB (2018) Efficient quantum information hiding for remote medical image sharing. IEEE Access 6:21075–21083
2. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Doctoral dissertation, University of Buckingham
3. Abdullatif FA, Abdullatif AA & al-Saffar A (2018) Hiding techniques for dynamic encryption text based on corner point. J Physics: Conf Series (Vol. 1003, no. 1, p. 012027). IOP Publishing
4. ALabaichi A, Al-Dabbas MAAAK, Salih A (2020) Image steganography using least significant bit and secret map techniques. Int J Electrical Comput Eng 10(1):2088–8708
5. Alam, S., Ahmad, T., & Doja, M. N. (2017). A novel edge based chaotic steganography method using neural network. In proceedings of the 5th international conference on Frontiers in intelligent computing: theory and applications (pp. 467–475). Springer, Singapore

6. Al-Husainy MAF, Uliyan DM (2019) A secret-key image steganography technique using random chain codes. Int J Technol 10(4):731–740
7. Al-Tamimi AGT, Alqobaty AA (2015) Image steganography using least significant bits (LSBs): a novel algorithm. Int J Comp Sci Inform Secur 13(1):1
8. Anushiadevi R, Praveenkumar P, Rayappan JBB, Amirtharajan R (2020) Reversible data hiding method based on pixel expansion and homomorphic encryption. Journal of Intelligent & Fuzzy Systems, (preprint), 1-14.
9. Arunkumar S, Subramaniyaswamy V, Vijayakumar V, Chilamkurti N, Logesh R (2019) SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. Measurement 139:426–437
10. Atawneh S, Almomani A, Al Bazar H, Sumari P, Gupta B (2017) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimed Tools Appl 76(18): 18451–18472
11. Bower A, Insoft R, Li S, Miller SJ, Tosteson P (2015) The distribution of gaps between summands in generalized Zeckendorf decompositions. J Comb Theory, Series A 135:130–160
12. Fadhel S, Shafry M, Farook O (2017) Chaos image encryption methods: a survey study. Bull Electrical Eng Inform 6(1):99–104
13. Fadhil AM (2016). Bit inverting map method for improved steganography scheme. Diss. Universiti Teknologi Malaysia.
14. Gambhir A, & Arya R (2019) Performance analysis and implementation of DES algorithm and RSA algorithm with image and audio steganography techniques. In computing, communication and signal processing (pp. 1021–1028). Springer, Singapore
15. Grajeda-Marín IR, Montes-Venegas HA, Marcial-Romero JR, Hernández-Servín JA, Muñoz-Jiménez V, Luna GDI (2018) A new optimization strategy for solving the fall-off boundary value problem in pixel-value differencing steganography. Int J Pattern Recognit Artif Intell 32(01):1860010
16. Grajeda-Marín IR, Montes-Venegas HA, Marcial-Romero JR, Hernández-Servín JA, Muñoz-Jiménez V, Luna GDI (2018) A new optimization strategy for solving the fall-off boundary value problem in pixel-value differencing steganography. Int J Pattern Recognit Artif Intell 32(01):1860010
17. Gutub A, Al-Shaarani F (2020) Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. Arab J Sci Eng 45(4):2631–2644
18. Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung KH (2018) Image steganography in spatial domain: a survey. Signal Process Image Commun 65:46–66
19. Jouini L, Ouannas A, Khennaoui AA, Wang X, Grassi G, Pham VT (2019) The fractional form of a new three-dimensional generalized Hénon map. Adv Diff Equa 2019(1):1–12
20. Jumanto J (2018) An enhanced LSB-image steganography using the hybrid canny-Sobel edge detection. Cybern Inf Technol 18(2):74–88
21. Kadhim IJ, Premaratne P, Vial PJ, Halloran B (2019) Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing 335:299–326
22. Kadhim IJ, Premaratne P, Vial PJ (2020) High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. Cogn Syst Res 60:20–32
23. Kumar R, Singh H (2020) Recent trends in text steganography with experimental study, In handbook of computer networks and cyber security (pp. 849–872). Springer, Cham
24. Kumar V, Kumar D (2018) A modified DWT-based image steganography technique. Multimed Tools Appl 77(11):13279–13308
25. Kuo WC, Wang CC, Hou HC (2016) Signed digit data hiding scheme. Inf Process Lett 116(2):183–191
26. Laishram D, Tuithung T (2021) A novel minimal distortion-based edge adaptive image steganography scheme using local complexity. Multimed Tools Appl 80(1):831–854
27. Li D, Deng L, Gupta BB, Wang H, Choi C (2019) A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. Inf Sci 479:432–447
28. Li J, Yu C, Gupta BB, Ren X (2018) Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. Multimed Tools Appl 77(4):4545–4561
29. Liao X, Yu Y, Li B, Li Z, Qin Z (2019) A new payload partition strategy in color image steganography. IEEE Trans Circ Syst Video Technol 30(3):685–696
30. Luo X, Liu F, Yang C, Lian S, Zeng Y (2012) Steganalysis of adaptive image steganography in multiple gray code bit-planes. Multimed Tools Appl 57(3):651–667
31. Mahana SK, & Aggarwal RK (2019). Image steganography: Analysis & Evaluation of secret communication. In proceedings of international conference on sustainable computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.
32. Mukherjee N, Paul G, Saha SK, Burman D (2020) A PVD based high capacity steganography algorithm with embedding in non-sequential position. Multimed Tools Appl 1–31

33. Nayak R (2015) Steganography with BSS-RSA-LSB technique: a new approach to steganography. IJSEAT 3(5):187–190
34. Nguyen TD, Arch-Int S, Arch-Int N (2016) An adaptive multi bit-plane image steganography using block data-hiding. Multimed Tools Appl 75(14):8319–8345
35. Nikam VP, Dhande SS (2019) Extended Fibonacci series for selection of carrier samples in data hiding and extraction. In international conference on intelligent data communication technologies and internet of things (pp. 40-50). Springer, Cham.
36. Nisha CD, Monoth T (2020) Analysis of spatial domain image steganography based on pixel-value differencing method. In soft computing for problem solving (pp. 385–397). Springer, Singapore.
37. Nyeem H (2017) Reversible data hiding with image bit-plane slicing. In 2017 20th international conference of computer and information technology (ICCIT) (pp. 1-6). IEEE.
38. Pradhan A, Sekhar KR, Swain G (2018) Digital image steganography using LSB substitution, PVD, and EMD. Math Probl Eng 2018:1–11
39. Prasad S, & Pal AK (2019). 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
40. Ramu P, Swaminathan R (2016) Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization. Expert Syst Appl 49:123–135
41. Rao CS, Devi VB (2016) Comparative analysis of HVS based robust video watermarking scheme, In microelectronics, electromagnetics and telecommunications (pp. 103–110). Springer, New Delhi
42. Rawat R, Singh B, Sur A, Mitra P (2020) Steganalysis for clustering modification directions steganography. Multimed Tools Appl 79(3):1971–1986
43. Sahu AK, Swain G (2019) An optimal information hiding approach based on pixel value differencing and modulus function. Wirel Pers Commun 108(1):159–174
44. Saidi M, Hermassi H, Rhouma R, Belghith S (2017) A new adaptive image steganography scheme based on DCT and chaotic map. Multimed Tools Appl 76(11):13493–13510
45. Seyyedi SA, Sadau V, Ivanov N (2016) A secure steganography method based on integer lifting wavelet transform. IJ Network Security 18(1):124–132
46. Shanthakumari R, Malliga S (2020) Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. Multimed Tools Appl 79(5):3975–3991
47. Som S, Mitra A, Palit S, Chaudhuri BB (2019) A selective bitplane image encryption scheme using chaotic maps. Multimed Tools Appl 78(8):10373–10400
48. Stojanovski T, Kocarev L (2001) Chaos-based random number generators-part I: analysis [cryptography]. IEEE Trans Circ Syst I: Fundamental Theory Appl 48(3):281–288
49. Subhedar MS, Mankar VH (2020) Secure image steganography using framelet transform and bidiagonal SVD. Multimed Tools Appl 79(3):1865–1886
50. Sun S (2016) A novel edge based image steganography with 2k correction and Huffman encoding. Inf Process Lett 116(2):93–99
51. Swain G (2018) High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis. Secur Commun Networks 2018:2018–2014
52. Swain G (2018) Adaptive and non-adaptive PVD steganography using overlapped pixel blocks. Arab J Sci Eng 43(12):7549–7562
53. Swain G (2019) Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arab J Sci Eng 44(4):2995–3004
54. Thomas E (2015) The Fibonacci sequence through a different lens (doctoral dissertation)
55. Vikranth BM, Momin MH, Mohsin SM, Rimal S, Pandey SR (2015) A survey of image steganography. J Emerg Technol Innov Res 2(4)
56. Wu DC, Tsai WH (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24(9–10):1613–1626
57. Yang Y, Zhang W, Liang D, Yu N (2018) A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images. Multimed Tools Appl 77(14):18043–18065
58. Yeung Y, Lu W, Xue Y, Chen J, Li R (2019) Secure binary image steganography based on LTP distortion minimization. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-7731-0
59. Zodpe H, Sapkal A (2020) An efficient AES implementation using FPGA with enhanced security features. J King Saud Univ Eng Sci 32(2):115–122