Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 08, No. 03, September 2022.

DATA HIDING TECHNIQUE FOR COLOR IMAGES USING PIXEL VALUE DIFFERENCING AND CHAOTIC MAP

Nisreen I. R. Yassin

(Received: 13-Feb.-2022, Revised: 12-Apr.-2022, Accepted: 27-Apr.-2022)

ABSTRACT

The huge advance in information technology and communication has resulted in the growing usage of digital networks, which consequently handed an important role to information security. Steganography is the art of hiding secret message bits into different multimedia data to provide the transferred information with security against unauthorized access. Most techniques applying the pixel value differencing (PVD) approach depend on the sequential embedding manner that lacks security. This study proposes a method that uses a complex chaotic map to randomly choose the coefficients for embedding a secret message. First, the cover image is transformed through integer wavelet transform (IWT). The embedding process starts in the highest-frequency band of IWT and continues to the next subbands according to the message size. Adaptive embedding is then performed depending on the intensity variation between pixel pairs using PVD and least significant bit substitution. The nonsequential embedding performed using the chaotic map makes the method more secure. The experimental results show that the proposed technique achieves a high peak signal-to-noise ratio with an improved capacity compared with other techniques.

KEYWORDS

Data hiding, Integer wavelet transform, Pixel value differencing, Chaotic map.

1. INTRODUCTION

Nowadays, a massive amount of information is being exchanged through the internet. Malicious users constantly try to steal information while performing transfers through that opened network. Information theft can cause systems to fail and countries to become defeated. Therefore, information security has become one of the most important topics to attract the attention of researchers. Cryptography [1]-[2], steganography [3], and watermarking [4] are the most popular technologies used to secure information. In cryptography, the sender changes the shape of the secret data, then using certain tools, the recipient returns the data back to its original shape. Although cryptography guarantees data confidentiality, the encrypted data can be traced and defined during transmission. This has resulted in an increase on the demand for data hiding techniques. Meanwhile, steganography is a technique of hiding secret data into another digital content, such as an image, a video, and an audio. The concealed secret data should not be seen by the naked eye [5]. Steganography is essential in security applications and in private and secure communication. Image steganography techniques are the most common, as image contains many redundant zones and is the most widely used media over the networks [6].

A steganography system consists of a cover image, which is the original image, the secret data hidden in the original image, a stego image that is the original image after hiding the secret data in it, and a security key for better security [3]. Image steganography techniques can be categorized into two types: spatial and frequency domain-based techniques. In the former, the secret data are directly concealed in the cover media. The most popular spatial domain technique is the least significant bit (LSB) substitution. In this approach, the LSBs of the cover media are replaced by the secret data bits [7]-[8]. Another technique is the pixel value differencing (PVD) technique, which hides secret bits in the difference between two consecutive pixels [9]-[10]. Spatial embedding techniques have high embedding capacity and imperceptibility with low computational time and robustness against attacks [11]. In frequency domain-based techniques, the secret data are embedded in the frequency transformation of the cover media. Transformation techniques have higher computational time and higher robustness against attacks but have a lower embedding capacity. There are many transformation techniques used in data hiding such as discrete cosine transform [12] and discrete wavelet transform [4]. The major defiance

N. Yassin is with Department of Systems and Information, Engineering and Renewable Energy Research Institute, National Research Centre, Cairo, Egypt. Email: nisreen.yassin20@gmail.com

in steganography is the preservation of the statistical properties and the visual quality of the cover image after the secret data have been embedded.

The quality of an image steganography system depends on three essential features, that is, image imperceptibility, payload capacity, and robustness. A tradeoff exists between these features; therefore, selecting the suitable embedding locations inside the cover image and identifying the amount of data to be embedded are important for achieving balance. Most steganography techniques select the cover image pixels sequentially to embed the secret data (e.g., PVD techniques). This manner of selection increases their vulnerability to statistical attacks. Chaotic map-based steganography techniques allow the embedment of the secret data in the cover image pixels in a nonsequential mode; however, they usually embed 1 bit of secret data into the cover image pixel, which limits the embedding capacity. Therefore, combining PDV techniques with chaotic map techniques could improve both security against statistical attacks and limited capacity. Embedding the secret data in sharp-edge regions is also less noticeable using human visual system compared with embedding them in smooth and uniform regions. Correspondingly, integer wavelet transform (IWT) is used to embed the secret data in the edge regions of the cover image.

This study proposes a new image steganography technique that applies PVD using a chaotic map for pixel selection. Unlike usual PVD methods, the proposed method embeds the secret data into nonsequential selected image pixels. Random pixel selection is performed using a complex chaotic map, which is very sensitive to the initial conditions and control parameters. The contributions of the proposed technique are as follows:

1- PVD is performed on the basis of a complex chaotic map, in which the selection of common pixels is completely random. Nonsequential embedding increases robustness to statistical attacks.

2- Adaptive embedding based on the contrast difference between the coefficient pairs is proposed.

3- High embedding capacity and efficiency are achieved with results that are comparable with those of other studies in the literature.

The remainder of this paper is organized as follows: Section 2 presents the related materials and methods; Section 3 introduces the proposed system; Section 4 discusses the experimental results; and Section 5 provides the conclusions.

2. RELATED MATERIALS AND METHODS

2.1 Related Materials

Many image steganography techniques in the literature consider spatial and frequency domains. The method of selecting pixels for embedding the secret data is important in attaining efficiency. Adaptive selection, edge detection selection, random selection, and color-dependent selection aim to increase the embedding capacity while preserving the good quality of the stego image. Both the PVD and LSB methods are used to embed the secret data in gray and colored images. The PVD method is a spatial domain method proposed by Wu et al. [9]. In this method, the gray cover image is divided into nonoverlapping blocks. The difference between the two successive pixels in each block is calculated and used to embed the secret data. The PVD method has been enhanced by many researchers to improve its hiding capacity [13]-[15]. In Paul et al. [16], PVD with nonsequential embedding was recently introduced. Pixel pairs were formed by taking the horizontal and vertical pixels from alternatively selected blocks. Although the embedding capacity was increased, the block selection depended on the predefined tables. Mandal et al. [17] proposed a data hiding technique based on the interpolation and difference expansion method. Although the proposed technique achieved a high embedding capacity, the gained peak signal-to-noise ratio (PSNR) was low.

Sahu et al. [18] proposed two reversible data hiding techniques for grayscale images to improve the embedding capacity without sacrificing the image quality. The first technique used LSB matching in dual images, whereas the second technique embedded the secret data using n-rightmost bit replacement. Solak and Altınışık [19] proposed a two-step data hiding scheme based on LSB. The secret information was first encrypted using keywords and shifting. Next, two types of adaptive LSB+3 were proposed to hide the encrypted data into the cover image. Solak [20] proposed a hybrid data hiding technique based on LSB substitution and enhanced modified signed digit algorithms. In the proposed technique, the n-adjacent pixels gained from the cover image and the k-least significant bits are used to embed the secret

data. Paul et al. [21] proposed a method for concealing the secret data in highly energetic pixels to increase robustness against statistical attacks. Liao et al. [22] investigated uniform and adaptive embedding. Setiadi [23] improved payload capacity in LSB using Canny and Sobel edge detection techniques. Feng et al. [24] proposed a method for minimizing the embedding distortion using the syndrome-trellis code. Chakraborty et al. [25] identified the edge areas using an edge predictor to conceal more secret data in sharper edges.

Liao et al. [26] proposed a method for adaptively partitioning the payload capacity among the red–green–blue channels of the cover image based on exploring the interchannel correlations. The method searches for high embedding probabilities and then modifies the pixel costs of the three channels. Liao et al. [27] also proposed a method for adaptively distributing the payload capacity among multiple images based on texture features for multiple-image steganography. They presented two strategies. The first strategy was based on the image texture complexity, whereas the second one was based on the distortion distribution. Al-Qwider et al. [28] proposed a hybrid security system based on gathering cryptography and steganography techniques. The secret message and the stego key were first encrypted using the modified Jamal encryption algorithm. The encrypted message was then hidden in the least 3–3–2 bits of the red–green–blue components of the cover image. Laffont et al. [29] proposed an RGB image steganography technique based on the modulus function. Each pixel value was modified to conceal one digit of the secret data. Wang et al. [30] proposed a watermarking technique for color images based on discrete cosine transform and just noticeable distortion. Abraham et al. [31] proposed a color image watermarking scheme using spatial domain methods. Parah et al. [32] proposed a spatial domain watermarking technique based on inter block pixel difference.

Saraireh et al. [33] proposed an image steganography system based on Haar-DWT. First, the secret message was encrypted using the advanced encryption standard algorithm. Next, the encrypted message was inserted in the DWT subbands. Valandar et al. [34] proposed an image steganography method based on IWT and chaotic map. First, IWT was applied on the cover image. Subsequently, the coefficients were randomly selected using a modified logistic map. Valandar et al. [35] also proposed a steganography technique based on a three-dimensional (3D) sine chaotic map. The secret message was embedded in the LL subband of IWT of an RGB cover image using the random numbers generated from the map. This algorithm embedded only one secret bit in each pixel of the cover image, resulting in a low embedding capacity. Ghebleh et al. [36] proposed a steganography system that concealed the secret data in the lifted discrete wavelet transform of the cover image. The secret data were randomly scattered in the cover image using a 3D chaotic map. Last, Sharafi et al. [37] proposed a new hybrid chaotic map used to present an image steganography method. Wavelet transforms were applied on the cover and secret images using different types of shift operators to enhance resistance against different attacks.

2.2 Methods

2.2.1 IWT

Dealing with digital images requires IWT due to the nature of image pixels, which are integer samples. Wavelet transform outputs are floating point numbers, even if the inputs are integers. Wavelet coefficients are rounded to integers, resulting in errors during the reconstruction of the original image from its transform version. A perfect reconstruction is achieved by eliminating the rounding error using a lifting scheme [38]-[39]. If $\boldsymbol{a}$ and $\boldsymbol{b}$ are two consecutive pixels, IWT can be computed by first computing the difference between $\boldsymbol{a}$ and $\boldsymbol{b}$ and then using that difference to compute the average as described in Equation (1). The inverse lifting is described in Equation (2) [40].

$$d = a - b \quad , \; s = \frac{d}{2} + b \tag{1}$$

$$b = s - \frac{d}{2} \quad , \; a = d + b \tag{2}$$

2.2.2 Chaotic Map

Most hiding techniques use a chaotic behavior to securely embed the secret information in the cover data. Chaotic maps are sensitive to the primary state where small variations in the input may produce large variations in the output. In the proposed method, the complex chaotic map introduced by Ayubi et al. [41] is used to select the positions for the secret data embedment. It is represented in Equations (3)–(5) as follows:

$$[z_1(n+1) \equiv \left(\alpha * \left(z_1(n)/z_2(n)\right)^2 + c_1\right)]\text{CFOLD1} \quad (3)$$

$$[z_2(n+1) \equiv (\beta * (z_2(n)/z_1(n))^2 + c_2)]\ \text{CFOLD 1} \quad (4)$$

$$(z\ CFOLD\ 1) = z^{real}\ Mod1 + (z^{imj} Mod\ 1) \times 1i \quad (5)$$

where z_1, z_2, c_1 and c_2 are complex numbers and $\alpha\ and\ \beta$ are integer numbers between $[10, \infty]$. This chaotic map is used for color images, where the real and imaginary parts of z_1 represent the image coordinates. The real part of z_2 is the color channel. For more security, the imaginary part of z_2 can be used to encrypt the secret data.

3. PROPOSED SYSTEM

Steganography aims to suppress secret messages into digital media without triggering trepidation. Embedding secret data in sequential pixels makes the steganography technique weak against statistical attacks [42]. In this section, we present a steganography technique that utilizes PVD and LSB to embed the secret data into an RGB cover image. The usual PVD divides the cover image into sequential pixel blocks for embedding the secret data. Our proposed technique randomly selects pixels nonsequentially using a chaotic map. The details of the proposed technique are presented in the subsequent sections.

3.1 Preprocessing

The following preprocessing steps are performed before the embedding process:

Step 1. The steganography system inputs are a cover image C of size $M \times N \times 3$, random data with different sizes used as a secret message SM to be hidden in the cover image, and a secret key K.

Step 2. Initialize the chaotic map control parameters $(z_1, z_2, c_1, c_2, \alpha, and\ \beta)$.

Step 3. Extract the RGB color channels of C. IWT is applied on each $R, G, and\ B$ color channel of size $M \times N$. Four subbands $[LL, LH, HL, HH]$ of size $M/2 \times N/2$ are obtained for each color channel.

Step 4. Save the original sign of the IWT coefficients of the cover image as an array of $[1, -1]$ to be used in image restoration.

Step 5. Collect the same subbands of the transformed coefficients of the three color channels together in a cell array $\{HH_{R,G,B}; HL_{R,G,B};\ LH_{R,G,B}; LL_{R,G,B}\}$.

3.2 Embedding Process

Steganography techniques concentrate on the maximization of the embedding capacity without contributing any visual image degradation. Traditional PVD methods sequentially embed a secret message in adjacent pixels by dividing the cover image into blocks. This embedding manner increases the detection ability by tracing the pixels of each block. In the proposed technique, nonsequential embedding is performed through two steps. The first step ensures that all edges are specified by applying IWT. All IWT subbands are used to conceal the secret message; however, the embedding process starts in high-frequency subbands $[HH, HL, LH]$ that represent the image's edge information. In the second step, a chaotic map is used to randomly select pixels from the IWT subbands. A complex chaotic map, which is very sensitive to the initial conditions and control parameters, is used to increase security and randomness. Figure 1 depicts the embedding process. The detailed steps are presented as follows:

Step 1. Start with the cell $HH_{R,G,B}$. Initialize a flag array of 0s converted to 1s after embedding to avoid a repeated selection of coefficients.

Step 2. Two consecutive coefficients $p_{x.y.z}$ and $p_{x+1.y.z}$ are selected from the transformed coefficients of the selected cell using the position generated by the real and imaginary parts of z_1 of the complex chaotic map. The color channel of each selected coefficient is indicated by the real part of z_2.

Step 3. The difference d between the two coefficients $p_{x.y.z}$ and $p_{x+1.y.z}$ is computed. If the value of d is <15, which indicates low variations between the two consecutive coefficients, then the secret bits are embedded through LSB substitution. Three bits are embedded into each selected coefficient from the LSB direction by applying the XOR function between the secret message bits and the generated secret key to obtain the new $p_{x,y,z}^{`}$ and $p_{x+1,y,z}^{`}$ coefficients.

Step 4. If d is >15, PVD is used to conceal the secret bits. The number of secret bits embedded in the difference value d is specified by classifying the value of d into four groups (Table 1). The number of secret bits n and the corresponding lower bound l are obtained according to the d value. Start the embedding process using PVD by converting the secret bits n into the corresponding decimal value c.

1- A new difference $\boldsymbol{d'}$ is calculated as indicated in Equation (6). The absolute difference between the old and new differences is calculated to conceal the secret message in the difference values of the wavelet coefficients. A new value d'' is obtained using Equation (7) and used to acquire possible new wavelet coefficients as declared in Equations (8 and 9).

$$d' = l + floor(c/2) \tag{6}$$

$$d'' = floor\big((abs(d - d')/2)\big) \tag{7}$$

$$p\grave{}_{x,y,z} = p_{x,y,z} \pm d'' \tag{8}$$

$$p\grave{}_{x+1,y,z} = p_{x+1,y,z} \pm d'' \tag{9}$$

2- Two values of new coefficients are obtained for each original coefficient. The new coefficients $p\grave{}_{x,y,z}$ and $p\grave{}_{x+1,y,z}$ are selected as the values nearest to the original coefficients as indicated in Equation (10).

$$p\grave{}_{x,y,z} = \begin{cases} p_{x,y,z} + d'' & if\ \left|p_{x,y,z} - (p_{x,y,z} + d'')\right| < \left|p_{x,y,z} - (p_{x,y,z} - d'')\right| \\ p_{x,y,z} - d'' & otherwise \end{cases}$$

$$p\grave{}_{x+1,y,z} = \begin{cases} p_{x+1,y,z} + d'' & if\ \left|p_{x+1,y,z} - (p_{x+1,y,z} + d'')\right| < \left|p_{x+1,y,z} - (p_{x+1,y,z} - d'')\right| \\ p_{x+1,y,z} - d'' & otherwise \end{cases} \tag{10}$$

The newly obtained coefficients $p\grave{}_{x,y,z}$ and $p\grave{}_{x+1,y,z}$ are referred to as the stego coefficients. Their values must be between 0 and 255.

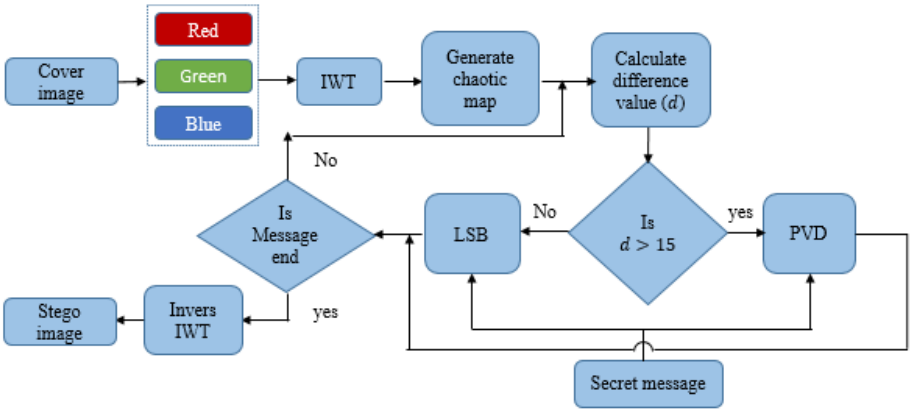

Figure 1. Embedding process of the proposed method.

Step 5. Steps 2–4 are repeated until the secret message bits are embedded. If the secret message has not ended, and all possible pairs in $HH_{R,G,B}$ have been selected, the embedding process restarts from step 1 using the next cell $HL_{R,G,B}$ and so on for cells $LH_{R,G,B}$ and $LL_{R,G,B}$. $LL_{R,G,B}$ is a low-frequency subband; hence, the number of bits in Table 1 is reduced by only 1 bit in the case of PVD embedding to minimize the distortion in this band.

Table 1. Difference groups and corresponding number of secret bits.

Difference Groups [l-u]	G_1 [16-31]	G_2 [32-63]	G_3 [64-127]	G_4 [128-255]
No. of secret bits	4	5	6	7

3.3 Postprocessing

The embedding process is completed by ending the message or by selecting all coefficient pairs in all subbands.

Pseudo-code 1: Embedding process

Input: Cover image C, Secret message SM, Secret key K, Initial values $z_1, z_2, c_1, c_2, \alpha, \beta$.
Output: Stego image I′

(R, G, B) ⟵ C % RGB color channels
[LL, LH, HL, HH] ⟵ IWT [(R, G, B)] % IWT subbands
[a b] ⟵ size(LL) % height and width of subbands
for each R, G, B
  if [LL, LH, HL, HH] < 0 then
    sign ⟵ -1 else sign ⟵ 1
  end
end
bandcell ⟵ $\{HH_{R,G,B}; HL_{R,G,B}; LH_{R,G,B}; LL_{R,G,B}\}$
[h w d] ⟵ size($HH_{R,G,B}$)
for counter =1 to 4
  bandnew ⟵ bandcell(counter)
  flag ⟵ zeros(h, w, d)
  while $s < SM$ do
    $z_1 \longleftarrow (\alpha * (z_1/z_2)^2 + c_1)$
    $z_1 \longleftarrow \mathrm{mod}\left(\left(real(z_1)\right), 1\right) + \mathrm{mod}\left(\left(imag(z_1)\right), 1\right)$*1i
    $z_2 \longleftarrow (\beta * (z_2/z_1)^2 + c_2)$
    $z_2 \longleftarrow \mathrm{mod}\left(\left(real(z_2)\right), 1\right) + \mathrm{mod}\left(\left(imag(z_2)\right), 1\right)$*1i
    x ⟵ $\mathrm{mod}(round(real(z_1) \times 10^{14}), h)$
    y ⟵ $\mathrm{mod}(round(imag(z_1) \times 10^{14}), w)$
    z ⟵ $\mathrm{mod}(round(real(z_2) \times 10^{14}), d) + 1$
    if flag(x, y, z) == 0 && flag (X+1, y, z) == 0 then
      p_1 ⟵ abs(bandnew(x, y, z))
      p_2 ⟵ abs(bandnew(x + 1, y, z))
      $diff$ ⟵ abs($p_1 - p_2$)
        if $diff > th$ then
          [p_{1new} p_{2new} s] ⟵ pvdembed($SM, diff, s, p_1, p_2$) % Apply Eqs.(6:10)
        else
          [p_{1new} p_{2new} s] ⟵ lsbembed(SM, s, p_1, p_2) % 3-LSb replacement
        end
      bandnew(x, y, z) ⟵ p_{1new}
      bandnew(x + 1, y, z) ⟵ p_{2new}
    end
    flag(x, y, z) ⟵ 1, flag(x+1, y, z) ⟵ 1
  end
  bandcell(counter) ⟵ bandnew
end
Reconstruct image
Apply inverse IWT
Get stego image I′

Step 1. The image is reconstructed after the embedding process. The original sign array is then used to give every stego coefficient its original sign by multiplying element-by-element the absolute of the stego array $I^{`}$ and the original sign array I as follows:

$$I^{`}(x,y,z) = abs\left(I^{`}(x,y,z)\right) * I(x,y,z) \tag{11}$$

Step 2. Finally, apply inverse IWT to obtain the stego image $I^{`}$. Pseudo-code 1 illustrates the embedding process in details.

3.4 Extraction Process

The same chaotic map initial conditions and secret key used in the embedding process are required to successfully extract the secret message. The extraction process starts with reading the stego image and transforming it into IWT. The chaotic map is then initialized, and a flag matrix is formed to prevent coefficient reselection. Figure 2 depicts the extraction process. The extraction steps are summarized as follows:

Step 1. The stego image is frequency-transformed using IWT. The chaotic map is initialized. Two consecutive coefficients ($p_{x.y.z}$ and $p_{x+1.y.z}$) are selected using the initialized chaotic map.

Step 2. The difference between the two coefficients d is computed. Three bits are directly extracted from the rightmost direction of the coefficients if d is <15.

Step 3. The lower bound l is identified according to the range of the difference value if d is >15 (Table 1). The decimal value of the secret bits is calculated as follows:

$$c = 2(d - l) \tag{12}$$

Finally, the secret binary bits are obtained by transforming the decimal value c into the binary form and concatenating all of them to acquire the secret message back. Pseudo-code 2 illustrates the extraction process.

Pseudo-code 2: Extraction process

Input: Stego image I′, Secret message size, Secret key K, Initial values $z_1, z_2, c_1, c_2, \alpha, \beta$.
Output: Secret message

(R, G, B) ⟵ I′ % RGB color channels
[LL, LH, HL, HH] ⟵ IWT [(R, G, B)] % IWT subbands
bandcell ⟵ $\{HH_{R,G,B};\ HL_{R,G,B};\ LH_{R,G,B};\ LL_{R,G,B}\}$
[h w d] ⟵ size ($HH_{R,G,B}$)
for counter =1 to 4
  flag ⟵ zeros (h, w, d)
  while $s < SM$ do
    z_1 ⟵ $(\alpha * (z_1/z_2)^2 + c_1)$
    z_1 ⟵ $\mathrm{mod}\left(\left(real(z_1)\right), 1\right) + \mathrm{mod}\left(\left(imag(z_1)\right), 1\right)$*1i
    z_2 ⟵ $(\beta * (z_2/z_1)^2 + c_2)$
    z_2 ⟵ $\mathrm{mod}\left(\left(real(z_2)\right), 1\right) + \mathrm{mod}\left(\left(imag(z_2)\right), 1\right)$*1i
    x ⟵ $\mathrm{mod}(round(real(z_1) \times 10^{14}), h)$
    y ⟵ $\mathrm{mod}(round(imag(z_1) \times 10^{14}), w)$
    z ⟵ $\mathrm{mod}(round(real(z_2) \times 10^{14}), d) + 1$
    if flag(x, y, z)== 0 && flag(x + 1, y, z) == 0 then
      p'_1 ⟵ abs(bandcell(x, y, z))
      p'_2 ⟵ abs(bandcell(x + 1, y, z))
      $diff$ ⟵ p'_1 - p'_2
        if $diff > th$ then
          extract using Table 1 and Eq. (12)
        else
          extract 3-LSB from each p'_1 and p'_2
        end
    end
    flag(x, y, z) ⟵ 1, flag(x+1, y, z) ⟵ 1
  end
end

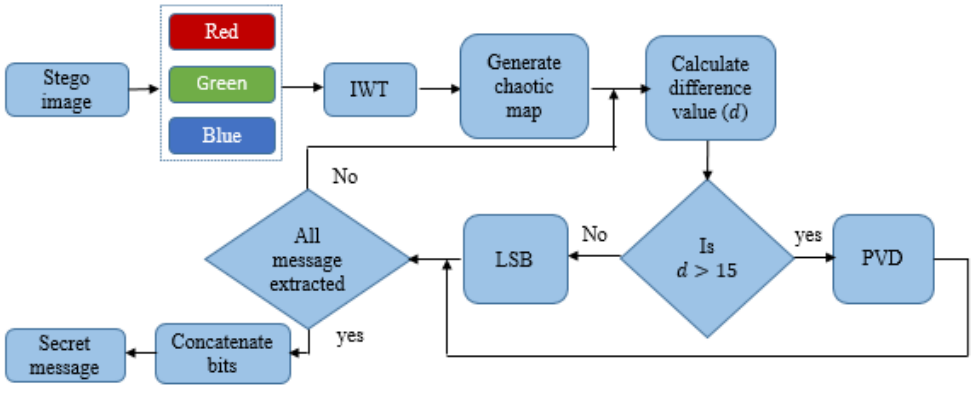

Figure 2. Extraction process of the proposed method.

4. EXPERIMENTAL RESULTS

Many experiments were conducted to evaluate the performance of the proposed technique. Matlab®2017 software on an Intel®Core™i5 CPU at 3.10 GHz computer was used for the simulation process. Standard color images (4.2.01, Lena, baboon, pepper, boat, and house) measuring 512 × 512, which were downloaded from the SIPI image database [43] were used to evaluate and compare the results of the proposed technique with those of the other existing steganography techniques. Figure 3 illustrates the cover images. Random data with different sizes were used as the secret messages.

Three standard metrics were used to evaluate the performance of any proposed steganography technique. The first metric is the embedding efficiency that evaluates the stego image quality. The second one is the payload embedding capacity defined as the amount of secret bits that can be hidden into the cover image. The third metric is the technique's robustness against different image processing operations and attacks.

- Embedding Efficiency Evaluation

The embedding efficiency is assessed using the PSNR, mean square error (MSE), and structural similarity index measure (SSIM) [4, 44]. The PSNR measures the difference between the cover image and its stego version and is computed using Equation (13). The MSE is the error between cover and stego images obtained using Equation (14). The system quality increases as long as the PSNR increases and the MSE decreases.

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right) \tag{13}$$

$$MSE = \frac{1}{M\times N\times 3}\sum_{i=1}^{M}\sum_{j=1}^{N}[I`(i,j) - I(i,j)]^2 \tag{14}$$

where, I is the cover image of size $M \times N \times 3$ and $I`$ is the stego image.

Although the MSE and PSNR measure the absolute error between two images, the SSIM [35] measures the structural similarity between two images and is calculated by Equation (15).

$$SSIM(I, I`) = (2u_x u_y + c_1)(2\sigma_{xy} + c_2)/(u_x^2 + u_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2) \tag{15}$$

where, x and y are two windows of common size; u_x and u_y are the averages of x and y, respectively; σ_{xy} is the co-variance of x and y; σ_x^2 is the variance of x; σ_y^2 is the variance of y; and c_1 and c_2 are two variables used to stabilize the division with a weak denominator.

SSIM result is a value between 0 and 1, where 0 indicates no structural similarity, whereas 1 indicates full structural similarity. Table 2 presents the MSE, PSNR, and SSIM values for some test images at different values of embedding capacities. The proposed technique achieved a high PSNR (i.e., above 50 dB for 125-kB embedding capacity). The achieved PSNR was greater than 30 dB, which is the PSNR threshold [45]. All achieved SSIM values were approximately 1, indicating the quality of the proposed system. Figure 4 shows the stego images after concealing 1,472,164 secret bits. The stego images clearly showed no degradation and were visually identical to the cover images, from which the naked eye cannot observe any difference between the cover and stego images. In summary, the proposed technique exhibited a good embedding efficiency.

Table 2. Results of the PSNR, MSE, and SSIM.

Cover image	**39kB**			**116kB**			**125kB**			**192kB**		
	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM
4.2.01	56.46	0.14	0.99	51.76	0.43	0.99	51.43	0.46	0.99	49.54	0.72	0.99
Lena	57.12	0.12	0.99	52.24	0.38	0.99	51.94	0.41	0.99	50.12	0.63	0.99
baboon	52.82	0.33	0.99	48.15	0.99	0.99	47.86	1.06	0.99	46.01	1.62	0.99
pepper	56.85	0.13	0.99	52.21	0.39	0.99	51.89	0.420	0.99	50.00	0.64	0.99
boat	56.09	0.15	0.99	51.26	0.48	0.99	50.95	0.52	0.99	49.15	0.79	0.99
house	56.53	0.14	0.99	51.77	0.43	0.99	51.45	0.46	0.99	49.58	0.71	0.99

Figure 3. Standard cover images: 4.2.01, Lena, baboon, pepper, boat, and house (left to right).

Figure 4. Stego images: 4.2.01, Lena, baboon, pepper, boat, and house (left to right).

- Embedding Capacity Evaluation

The embedding capacity is the maximum amount of secret data that can be hidden in the cover without being noticed. It is also known as the embedding rate that can be calculated using Equation (16).

$$Embedding\ rate = \frac{Number\ of\ embedded\ secret\ bits}{Image\ size} \quad (16)$$

Figure 5 illustrates the efficiency of the proposed system at different embedding rates, where the PSNR is plotted at the embedding rates of 20%, 40%, 60%, 80%, and 100% for three colored images (i.e., Lena, pepper, and house). For the 20% embedding rate, the PSNR was greater than 45 dB and decreased as the embedding rate increased until approximately 35 dB at 100% embedding rate (1,578,972 bits). The proposed system achieved considerably high embedding rates with an acceptable PSNR. Additionally, the used images exhibited approximately the same results according to different embedding rates.

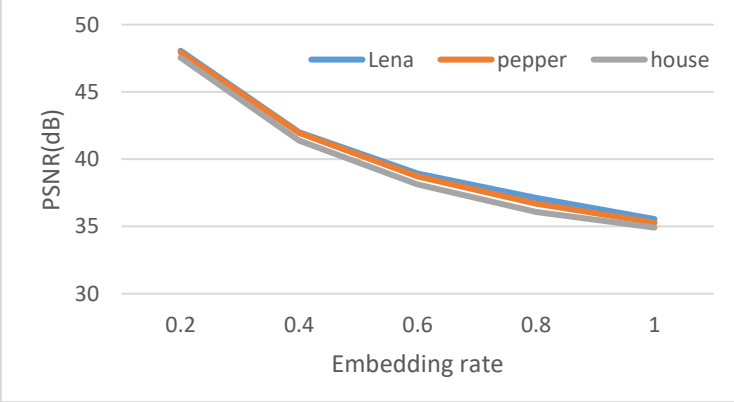

Figure 5. Efficiency of the proposed system at different embedding rates.

- Robustness Evaluation

Figure 6 shows a histogram plot of the RGB color channels of the Lena cover image and the Lena stego image to determine the robustness of the proposed system against a histogram analysis. The histogram form for the three colored channels was conserved with very minimal changes. Figure 7 plots and fits the histogram of the difference between the cover and stego images as a normal distribution. The histogram of the difference values is concentrated around zero, indicating the robustness of the proposed system.

We used the Virtual Steganographic Laboratory (VSL) tool to test the proposed technique against steganalysis. The VSL tool is a steganography detection software used to apply the RS analysis, which estimates the concealed message's length. Figure 8 presents a sample report of the VSL tool showing the name of the input stego image and the corresponding detected message size in bytes. For the used images, the ratio between the average detected capacities to the actual capacity was computed. The obtained detection ratio was 20%, indicating the robustness of the proposed technique.

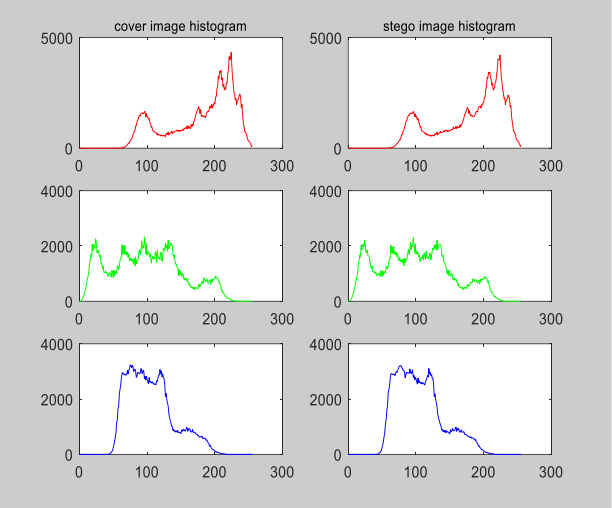

Figure 6. Histogram of the Lena cover and stego images.

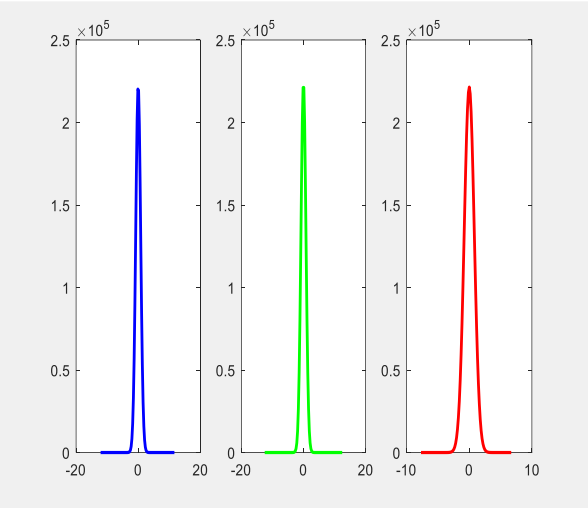

Figure 7. Histogram of the difference between the Lena cover and stego images.

	A	B	C	D	E
1	1	LSB-RS	E:\testfolder_2\stego_Lena.png	512x512	Estimated message size [B]:773.1707724709962
2	2	LSB-RS	E:\testfolder_2\stego_Baboon.png	512x512	Estimated message size [B]:5891.683894314265
3	3	LSB-RS	E:\testfolder_2\stego_boat.png	512x512	Estimated message size [B]:1446.253526212815
4	4	LSB-RS	E:\testfolder_2\stego_house.png	512x512	Estimated message size [B]:1025.732603759307
5	5	LSB-RS	E:\testfolder_2\stego_Pepper.png	512x512	Estimated message size [B]:9317.495468119538
6	6	LSB-RS	E:\testfolder_2\stego_4.2.01.png	512x512	Estimated message size [B]:1777.9765822308163
7	7	LSB-RS	E:\testfolder_2\stego_jet.png	512x512	Estimated message size [B]:557.4034805599041

report

Figure 8. VSL sample report.

Computational Complexity

Computational complexity is important for evaluating the performance of any algorithm. It depends on the processor speed, available memory, and algorithm type. Table 3 presents the processing time of the proposed technique. The obtained results were compared with those proposed in [34] using the same cover image and embedding capacities.

Table 3. Processing time of the proposed technique.

Cover image	Secret message (kb)	Embedding time (s)		Extraction time (s)	
		Proposed technique	[34]	Proposed technique	[34]
Lena	Random data (39)	0.286129	0.827536	0.138638	0.469742
Lena	Random data (116)	0.628100	1.568793	0.487249	1.391331
Lena	Random data (125)	0.656901	1.596450	0.419632	1.403308

- Comparison of the Proposed Technique with Other Techniques

Some algorithms based on IWT that used the same color images and implemented chaotic maps were used to compare our technique with that in the literature. Table 4 shows the comparison results of the proposed technique and those proposed in [34] and [36] according to the embedding capacity, PSNR, and SSIM. Although the PSNR values reported in [34] and [36] were higher than those achieved by the proposed system at the same payload capacity, we found a high amelioration in the embedding capacity; that is, 1,578,972 bits can be hidden without any degradation in the image with approximately 38 dB.

Table 5 presents the comparison results of the proposed technique and those presented in [35] and [29]. In [35], 77,244 bits were embedded as the secret data in the cover images (Lena, baboon, pepper, and jet). Compared with the technique presented in [35], the proposed technique achieved higher PSNR and SSIM values for Lena, pepper, and jet but lower values for baboon. In [29], different sizes of secret data were embedded into the cover images. Table 5 shows that the results accomplished using the proposed technique were greater than or approximately equal to those achieved in [29].

Table 4. Comparison of the proposed technique with methods in the literature.

Cover image	**Proposed technique**			**[34]**			**[36]**		
	capacity	PSNR	SSIM	capacity	PSNR	SSIM	capacity	PSNR	SSIM
Lena	125 kb	51.944	0.9998	125 kb	52.998	0.9979	125 kb	56.135	0.9997
baboon	125 kb	47.868	0.9994	125 kb	52.993	0.9993	NA	NA	NA

Table 5. Comparison of the proposed technique with methods in the literature.

Cover image	Secret size (bits)	**Proposed technique**		**[35]**		Secret size (bytes)	**Proposed technique**		**[29]**	
		PSNR	SSIM	PSNR	SSIM		PSNR	SSIM	PSNR	SSIM
Lena	77244	54.1489	0.9999	51.3761	0.9984	83654	41.5132	0.9980	41.2968	NA
baboon	77244	49.9544	0.9997	52.4228	0.9991	91286	41.2815	0.9949	40.8535	NA
pepper	77244	54.0779	0.9999	52.3907	0.9986	78612	42.0032	0.9981	41.5641	NA
jet	77244	53.7585	0.9998	51.9846	0.9980	81851	41.1846	0.8893	41.2968	NA

With relevance to the PVD-based methods, the proposed technique was compared with that in [46] as a PVD-based method that uses the same color images with the same size. Table 6 shows that the proposed technique achieved a higher PSNR compared with that in [46] under the same payload capacities for all images. Table 7 presents a comparison of the proposed technique and the algorithms in [22], [24], [25], [21] and [9] according to the payload embedding capacity and the PSNR. The proposed technique had a higher embedding capacity with an acceptable PSNR than the other algorithms. The maximum payload that can be embedded without any image degradation was 2bpp with 37.5 dB PSNR, which proved the superiority of the proposed technique.

Although many techniques apply PVD and achieve a higher capacity than the proposed technique, most of them implement the commonly used sequential embedding approach. On the contrary, the proposed technique selects the pixel pairs in a fully nonsequential manner using a chaotic map that leads to increased security. Embedding the secret data in the IWT subbands also ensures complete reversibility and prefect reconstruction of data.

Table 6. Comparison of the proposed technique with PVD-based methods.

Image 512x512x3	**Payload capacity**	**Embedding rate (bpp)**	**PSNR**	
			PVD [46]	**proposed**
Lena	810757	1.030	37.13	40.31
baboon	918877	1.168	34.95	36.87
pepper	812986	1.033	36.74	39.81
jet	818887	1.041	36.36	39.24
boat	851837	1.083	36.03	38.66
house	834866	1.061	36.57	39.01
Average	841368	1.069	36.30	38.98

Table 7. Average embedding rate (AER) and the PSNR comparison.

Method	**AER (bpp)**	**PSNR (dB)**
Liao et al. [22]	≤ 1	44.72
Feng et al. [24]	≤ 1	26.83
Soumendu et al. [25]	≤ 1	30.0
Paul et al. [21]	≤ 1	38.54
Wu et al. [9]	1.56	39.06
Proposed technique	2.00	37.54

Table 8. Comparing PSNR values using binary secret logos.

Binary logo size	**9×(85×85)**		**64×64**			**3×(64×64)**	
	Proposed	[37]	Proposed	[30]	[31]	Proposed	[32]
Lena	54.9103	54.4578	66.8594	45.4018	53.35	62.4419	40.58
baboon	51.6294	52.1523	63.0485	43.8262	53.35	58.2916	39.60

Table 8 shows a comparison of the proposed technique with recent techniques using binary secret logos. The results indicate that the proposed technique had the superiority according to PSNR and embedding capacity.

5. CONCLUSIONS

In this study, we proposed a new image steganography technique based on the nonsequential application of the PVD approach using a complex chaotic map to withstand statistical attacks. We performed adaptive embedding using LSB or PVD to minimize the embedding distortion. The embedding process started in the highest-frequency detail band of IWT and continued to the other bands until the secret data embedding was completed.

Many experimental tests were conducted to evaluate the performance of the proposed technique. In summary, we obtained the following conclusions:

- According to the embedding efficiency test, the stego image looked identical to the cover image, from which the naked human eye cannot observe any difference between the two images even at high embedding rates.

- The robustness of the proposed technique was achieved. We observed no difference between the histograms of the cover images and the corresponding stego images. Moreover, only 20% of the embedded secret data could be detected using the VSL tool.

- In comparison with other techniques, the proposed technique exhibited a good performance and a good balance between the embedding capacity and imperceptibility.

CONFLICT OF INTERESTS

The author declares that no conflict of interest.

ACKNOWLEDGEMENTS

The author appreciates National Research Centre (NRC), Cairo, Egypt for funding this study through research project No (12010501).

REFERENCES

[1] H. M. Ghadirli, A. Nodehi and R. Enayatifar, "An Overview of Encryption Algorithms in Color Images," Signal Processing, vol. 164, pp. 163-185, 2019.

[2] P. Ayubi, S. Setayeshi and A. M. Rahmani, "Deterministic Chaos Game: A New Fractal Based Pseudo-random Number Generator and Its Cryptographic Application," Journal of Information Security and Applications, vol. 52, p. 102472, 2020.

[3] I. J. Kadhim, P. Premaratne, P. J. Vial and B. Halloran, "Comprehensive Survey of Image Steganography: Techniques, Evaluations and Trends in Future Research," Neurocomputing, vol. 335, pp. 299-326, 2019.

[4] E. M. El Houby and N. I. Yassin, "Wavelet-hadamard Based Blind Image Watermarking Using Genetic Algorithm and Decision Tree," Multimedia Tools and Applications, vol. 79, pp. 28453-28474, 2020.

[5] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, vol. 31, pp. 26-34, 1998.

[6] S. Nazari, A. M. Eftekhari-Moghadam and M. S. Moin, "A Novel Image Steganography Scheme Based on Morphological Associative Memory and Permutation Schema," Security and Communication Networks, vol. 8, pp. 110-121, 2015.

[7] Z. Xia, X. Wang, X. Sun and B. Wang, "Steganalysis of Least Significant Bit Matching Using Multi-order Differences," Security and Communication Networks, vol. 7, pp. 1283-1291, 2014.

[8] M. Afrakhteh and J. A. Lee, "Adaptive Least Significant Bit Matching Revisited with the Help of Error Images," Security and Communication Networks, vol. 8, pp. 510-515, 2015.

[9] D.-C. Wu and W.-H. Tsai, "A Steganographic Method for Images by Pixel-value Differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.

[10] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, "Image Steganographic Scheme Based on Pixel-value Differencing and LSB Replacement Methods," IEE Proceedings-Vision, Image and Signal Processing, vol. 152, pp. 611-615, 2005.

[11] H. Al-Dmour and A. Al-Ani, "A Steganography Embedding Method Based on Edge Identification and XOR Coding," Expert Systems with Applications, vol. 46, pp. 293-306, 2016.

[12] A. Saxena and F. C. Fernandes, "DCT/DST-based Transform Coding for Intra Prediction in Image/Video Coding," IEEE Transactions on Image Processing, vol. 22, pp. 3974-3981, 2013.
[13] A. K. Gulve and M. S. Joshi, "An Image Steganography Algorithm with Five pixel Pair Differencing and Gray Code Conversion," International Journal of Image, Graphics and Signal Processing, vol. 6, p. 12, DOI:10.5815/ijigsp.2014.03.02, 2014.
[14] A. K. Gulve and M. S. Joshi, "An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach," Mathematical Problems in Engineering, vol. 2015, DOI: 10.1155/2015/684824, 2015.
[15] G. Swain, "Two New Steganography Techniques Based on Quotient Value Differencing with Addition-subtraction Logic and PVD with Modulus Function," Optik, vol. 180, pp. 807-823, 2019.
[16] G. Paul, S. K. Saha and D. Burman, "A PVD Based High Capacity Steganography Algorithm with Embedding in Non-sequential Position," Multimedia Tools and Applications, vol. 79, pp. 13449-13479, 2020.
[17] P. C. Mandal, I. Mukherjee and B. N. Chatterji, "High Capacity Reversible and Secured Data Hiding in Images Using Interpolation and Difference Expansion Technique," Multimedia Tools and Applications, vol. 80, pp. 3623-3644, 2021.
[18] A. K. Sahu and G. Swain, "High Fidelity Based Reversible Data Hiding Using Modified LSB Matching and Pixel Difference," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 4, DOI: 10.1016/j.jksuci.2019.07.004, 2019.
[19] S. Solak and U. Altınışık, "Image Steganography Based on LSB Substitution and Encryption Method: Adaptive LSB+ 3," Journal of Electronic Imaging, vol. 28, p. 043025, DOI: 10.1117/1.JEI.28.4.043025, 2019.
[20] S. Solak, "High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms," IEEE Access, vol. 8, pp. 166513-166524, 2020.
[21] G. Paul, I. Davidson, I. Mukherjee and S. Ravi, "Keyless Steganography in Spatial Domain Using Energetic Pixels," Proc. of the International Conference on Information Systems Security (ICISS 2012), vol. 7671, pp. 134-148, 2012.
[22] X. Liao, Z. Qin and L. Ding, "Data Embedding in Digital Images Using Critical Functions," Signal Processing: Image Communication, vol. 58, pp. 146-156, 2017.
[23] D. Setiadi, "Improved Payload Capacity in LSB Image Steganography Uses Dilated Hybrid Edge Detection," J. King Saud Univ.-Comput. Inf. Sci., vol. 34, no. 2, DOI:10.1016/j.jksuci.2019.12.007, 2019.
[24] B. Feng, W. Lu and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 243-255, 2014.
[25] S. Chakraborty, A. S. Jalal and C. Bhatnagar, "LSB Based Non Blind Predictive Edge Adaptive Image Steganography," Multimedia Tools and Applications, vol. 76, pp. 7973-7987, 2017.
[26] X. Liao, Y. Yu, B. Li, Z. Li and Z. Qin, "A New Payload Partition Strategy in Color Image Steganography," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, pp. 685-696, 2019.
[27] X. Liao, J. Yin, M. Chen and Z. Qin, "Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 897-911, 2020.
[28] W. H. Al-Qwider and J. N. B. Salameh, "Novel Technique for Securing Data Communication Systems by Using Cryptography and Steganography," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 3, no. 2, pp. 110-130, 2017.
[29] A. Laffont, P. Maniriho, A. Ramsi, G. Guerteau and T. Ahmad, "Enhanced Pixel Value Modification Based on Modulus Function for RGB Image Steganography," Proc. of the 11th Int. Conf. on Information & Communication Technology and System (ICTS), 2017, pp. 61-66, Surabaya, Indonesia, 2017.
[30] J. Wang, W. B. Wan, X. X. Li, J. De Sun and H. X. Zhang, "Color Image Watermarking Based on Orientation Diversity and Color Complexity," Expert Systems with Applications, vol. 140, p. 112868, DOI: 10.1016/j.eswa.2019.112868, 2020.
[31] J. Abraham and V. Paul, "An Imperceptible Spatial Domain Color Image Watermarking Scheme," Journal of King Saud University-Computer and Information Sciences, vol. 31, no. 1, pp. 125-133, 2019.
[32] S. A. Parah, J. A. Sheikh, N. A. Loan and G. Bhat, "A Robust and Computationally Efficient Digital Watermarking Technique Using Inter Block Pixel Differencing," in Multimedia Forensics and Security, ed. Springer, pp. 223-252, 2017.
[33] S. M. Saraireh and A. M. Matarneh, "Higher Level Security Approach for Data Communication System Based on AES Cryptography and DWT Steganography," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 2, no. 3, pp. 179-193, 2016.
[34] M. Y. Valandar, P. Ayubi and M. J. Barani, "A New Transform Domain Steganography Based on Modified Logistic Chaotic Map for Color Images," Journal of Information Security and Applications, vol. 34, pp. 142-151, 2017.

[35] M. Y. Valandar, M. J. Barani, P. Ayubi and M. Aghazadeh, "An Integer Wavelet Transform Image Steganography Method Based on 3D Sine Chaotic Map," Multimedia Tools and Applications, vol. 78, pp. 9971-9989, 2019.
[36] M. Ghebleh and A. Kanso, "A Robust Chaotic Algorithm for Digital Image Steganography," Communications in Nonlinear Science and Numerical Simulation, vol. 19, pp. 1898-1907, 2014.
[37] J. Sharafi, Y. Khedmati and M. Shabani, "Image Steganography Based on a New Hybrid Chaos Map and Discrete Transforms," Optik, vol. 226, no. 2, p. 165492, 2021.
[38] N. I. R. Yassin and E. M. F. El Houby, "Image Steganography Technique Based on Integer Wavelet Transform Using Most Significant Bit Categories," International Journal of Intelligent Engineering and Systems, vol. 15, pp. 499-508, 2022.
[39] C. Liji, K. Indiradevi and K. A. Babu, "Integer-to-integer Wavelet TransformBased ECG Steganography for Securing Patient Confidential Information," Procedia Technology, vol. 24, pp. 1039-1047, 2016.
[40] A. La Cour–Harbo and A. Jensen, "Wavelets and the Lifting Scheme," Proc. of Encyclopedia of Complexity and Systems Science, pp. 10007-10031, DOI: 10.1007/978-0-387-30440-3_588, Springer New York, 2009.
[41] P. Ayubi, M. Jafari Barani, M. Yousefi Valandar, B. Yosefnezhad Irani and R. Sedagheh Maskan Sadigh, "A New Chaotic Complex Map for Robust Video Watermarking," Artificial Intelligence Review, vol. 54, pp. 1237-1280, 2021.
[42] N. Provos, "Defending against Statistical Steganalysis," Proc. of the 10th USENIX Security Symposium (USENIX Security 01), [Online], Available: https://www.usenix.org/conference/10th-usenix-security-symposium/defending-against-statistical-steganalysis, 2001.
[43] USC-SIPI Image Database, [Online], Available: http://sipi.usc.edu/database/database.php?volume=misc.
[44] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, vol. 13, pp. 600-612, 2004.
[45] N.-I. Wu and M.-S. Hwang, "Data Hiding: Current Status and Key Issues," IJ Network Security, vol. 4, pp. 1-9, 2007.
[46] S. Shen, L. Huang and Q. Tian, "A Novel Data Hiding for Color Images Based on Pixel Value Difference and Modulus Function," Multimedia Tools and Applications, vol. 74, pp. 707-728, 2015.

ملخص البحث:

أدّى التّقدّم الهائل في تكنولوجيا المعلومات والاتّصالات الى استخدامٍ مُفرطٍ للشّبكات الرّقمية، الأمر الذّي يجعل أمن المعلومات له دور هامّ. لذا، عمدت بعض التّقنيات الى إخفاء رسائل سرّيّة في بيانات وسائل التّواصُل المختلفة باستخدام إمّا الحقْل الحيّزي أو الحقْل التّرددي لتوفير الأمان للمعلومات المنقولة. وتجدر الإشارة الى أنّ غالبية التّقنيات التي تطبّق طريقة التّفريق بين قِيم النُّقط (PVD) تعتمد على أسلوب التّضمين التّتابُعي، الأمر الذي يضرّ بأمْن المعلومات.

في الطّريقة المقترحة في هذا البحث، تُستخدم خريطة فوضوية معقّدة للاختيار العشوائي لأزواج العوامل من أجْل تضمين الرّسالة السّرّية. يتمّ أوّلاً تحويل صورة الغلاف باستخدام تحويل المويجات التّامّ (IWT). بعد ذلك، تبدأ عملية التّضمين في النّطاق التّردّدي الأعلى من تحويل المويجات التّامّ وتستمرّ الى النّطاقات الفرعية التالية. ويتمّ إجراء التّضمين التّكيّفي وفْق تغيُّر الشِّدة بين أزواج النُّقَط باستخدام التّفريق بين قِيم النُّقَط (PVD) واستبدال الأجزاء الأقلّ أهمّية (LSB).

ويجعل التّضمينُ غيْرُالتّتابعيِ الّذي يتمّ بواسطة الخريطة الفَوْضوية الطّريقةَ المقترحة أكثر أماناً. وقد بيّنت النّتائج التّجريبية أنّ التّقنية المقترحة في هذه الورقة حققت نسبة إشارةٍ الى ضجيج عالية إضافةً الى سِعة محسَّنة لدى مقارنتها بطرقٍ مُستخدَمة أُخرى.