Turkish Journal of Computer and Mathematics Education *Vol.21 No.14 (2020), 4693-* 4701

Research Article

Hiding Secret image and text in image based (DWT) and Chaos Theory

Doaa mahmood abass[1] , Assist. Prof. Dr. Ali Hussien Mary[2]

[1,2]Informatic Institute for postgraduate studies,Univecity of technology

Email [1] : ms201930538@iips.icci.edu.iq, Email [2]: alimary76@kecbu.uobaghdad.edu.iq

Article History: Received: 27July 2021; Revised: 14September 2021; Accepted: 15October 2021.

Abstract: Steganography is a hiding information which is the science and art of secret communication. It allows the transmission of confidential information and the concealment of the presence of the message itself in content such as video, audio or image to protect the information sent from intruders and unwanted recipients. In the past decade, a variety of researches have been conducted on schematics of steganography in both the spatial and transformation domain.

In this research, an image of steganography system that hides medical image and secret key inside another color cover image was proposed using a combination of Discrete Wavelet Transform Technique (DWT) , Particle Swarm optimization , and chaotic theory.

Matlab 2018 has been used to implement the proposed algorithm. Based on the performance indexes that are calculated for each method, all the proposed methods achieve a good performance. Thus, the proposed algorithms achieved the steganographic goals that are designed for this purpose.

Keywords: Steganography, Watermarking, Wavelet Transform (WT), DWT.

Introduction

Steganography can be defined as the art of hiding and transmitting data through conspicuous and innocuous carriers in an aim to conceal the existence of the data.

Although steganography is considered as an antique craft, yet the proem of computer technology has granted it a second fresh life. In fact, computer-based steganographic techniques have introduced many changes to digital covers to hide outlandish information into the native covers. Such datum could be a communicative one in the form of a text, binary files, or for supplying further information regarding the cover itself [1].

Moreover, the outstanding characters of steganography allowed it to own its place within security fields for the intentions of supplementing the cryptography instead of replacing it. Hiding a message through applying steganography methods can reduce the chance of detecting that message, and in case the message is encrypted, then this would provide an additional layer of security [2].

Therefore, some steganographic techniques are combining traditional cryptography along with steganography; where the sender will encrypt the secret message prior to the embedding process. As a matter of fact, such an amalgamation increases the security levels of the total communication process, as it is much complicated for an attacker to reveal the embedded ciphertext in a cover [3]

Literature review

Shuhui Chen, Zengqiang Chen and Zhuzhi Yuan,(2008) They suggested to use multi dimension Chaotic map as a key generator and cat map for permutation, their method designed to use both stream cipher and block cipher in order to produce encrypted video, first they used Logistic map and multi dimension system to generate pseudo-random encryption sequence, and to perform the encryption, the DC coefficient and some AC coefficient are selected from the input frame apply XOR operation between those coefficient and the chaotic sequence then using cat map for block cipher as pixel permutation. The use of Chaotic system ensure large key space and block cipher reduces the likelihood of the known plain text attack [4].

Hephzibah Kezia and Gnanou Florence Sudha (2008) in this encryption method, Logistic and Lorenz Chaotic systems are used in the key generation process. In this method each frame has its own key. Logistic map used to generate Chaotic sequence in iterative for each iterative the results of the Logistic map added to one of the Lorenz

system parameters this operation used to generate key for each frame and can improve the Chaotic sequence that produced from this system. To generate key sequence, they applied 4th Runge-Kutta and Lorenz system equation to get Chaotic sequence which used for encryption. The forthcoming video sequence is first divided into frames. for each frame a unique key is generated, based on the changing one of control parameters or initial values of the Lorenz system. Video frame is divided into blocks. The size of the blocks is chosen to be (8* 8). The block positions are changed according to the Chaotic key sequence. The experimental results show that the algorithm has high security with significant key sensitivity and large enough key space [5].

Nitin, et al. (2014) [6] presented a novel image steganography method that was done based on LSB and DCT coefficients that provide randomly scattered bits embedding directly inside the cover image. At first, the Discrete Cosine Transform (DCT) was applied on the cover image and then the secret image was hidden in LSB of the cover image in random locations based on an embedding threshold value. Then, the randomized pixel locations that are used to embed secret information were found using DCT coefficients. The whole performance evaluation of the algorithm showed an improvement on both the security and the invisibility of stego image.

Haar Wavelet Transform

The wavelet transformation is a mathematical method for translating images from the spatial to the frequency domain. The image is passed through E through the filters for high and low passes, respectively, to obtain the low and high frequencies. Wavelet splits the category and the category of approximations into specifics and translates signal analysis treaties. The transmission was received is investigated on a variety of scales and frequency bands Scaling and wavelet, which apply to high and low pass filters, have been added to DWT. The decomposition works by dividing time into two parts. In other words, half of the samples in a signal are sufficient to twice the frequency separation of the total signal [7]. In the Haar Wavelet Transform, the low frequency wavelet coefficient is calculated by taking half of the average of the two pixel values, whereas the high frequency coefficients are calculated by taking half of the average of the two pixel values.

For the same two pixels, there is a difference. There are two photographs of damnation in this set. WT decomposes the image into multiple sub-bands as the resolution approximation band or low-low (LL), detailed components, in addition to horizontal high-low (HL), vertical low-high (LH), and diagonal high-high (HH), as illustrated in Figure 1. The key information of the spatial domain image (smooth sections) is found in the low-frequency wavelet coefficients (approximation band), whereas the edge and texture features are usually found in the high-frequency sub-bands, such as LH, HL, and HH. The Haar wavelet's transformation is comparable to its inverse, which is seen as a distinguishing feature[7].

Figure (1) Haar Wavelet Transform

Chaos Theory

Chaotic systems have widely attracted the researchers in the field of computer security. Due to the properties of the chaotic systems that can be exploit in encryption techniques. Combining Chaotic systems with encryption

algorithms becomes very interesting subject because of the characteristic that chaotic system over which make those systems suitable to be use in digital encryption [8].
Many challenges in the traditional encryption were the motivation for exploring the chaotic based encryption. With the development of chaotic encryption systems, they become used in wide range of applications and fields such as military communication and private data encryption [9].
The original development fields of Chaos theory were mathematics and physics. Chaos is a kind of complex dynamic systems and produced from nonlinear continuous systems or discrete systems. Chaotic systems are extremely sensitive to the initial conditions and also highly sensitive to the parameters of the discrete or continues chaotic systems with pseudo randomize property, such properties are suitable to be used for encryption [10].

Proposed method

The proposed algorithm is based on chaotic algorithm by process by scattering the image pixels

3.3.1Embedding process

The embedding process can be applied as follows:

1st step: Divide the image into color layers (Red, Green, and Blue).

2nd step: Apply DWT for each color of the input image and the Approximate, Horizontal, Diagonal and Vertical sub bands are obtained

3rd step: DCT is applied for each sub band that obtained in the 2nd step

DCT (I ,j) = $\frac{2}{N}$ C(i) C(j) $\sum_{X0}^{N-1} \sum_{Y=0}^{N-1} pixel(x,y)$ …….(2)

$$\text{Cos}\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1j\pi)}{2n}\right]$$

where:

• DCT (i,j) represents the value of the DCT at the point of coordinates (i, j) in the block of 8x8 pixels.

• Pixel (x, y) represents the value of the pixel of coordinates (x, y) in the block of the original image of 8x8 pixels

4th step: in this, the coordinates of pixels will be changed by applying the Chaotic on the pixels of images that result from the previous step

Pixel position transform (changing pixel coordinate)

This is the type of digital image encryption processes, which

is the cipher text generated by changing the pixels positions instead of

changing its values. It is achieved by implementing a two dimensional

chaotic map to transfer each pixel position of the plaintext to a new

position to generate the cipher image.

The input is number of row and column

- ***Suppose the initial value***

c = 4;

B = .5;

intial _value= 0.15;

List(1) = B - c *(intial_value^2);

-apply the chaotic algorithm

For i= 2: row*collum

Arr(i)= B – C*pixel_Order(i-1).^2;]

End

where:

C and B is Parameter

5th step: Divide the cover image into RED, Green, Blue color layers and apply DWT for each layer.

6th step: a color layer of hidden image will be embedded into its corresponding layer of cover image .

Seventh stage:

secret text Selection and Processing Stage:

At this stage, the previous stages were repeated by adding the secret text according to the following steps:

The secret text is read first, then the letters are converted to ASCII code and ASCII is converted to binary. After which they are stored in lists.

After completing the above process, the length of the text is calculated, and the length of the strings is entered at the beginning of the list. Then the DWT and the chaotic process of scattering the text are performed. Finally, the list is stored in (LH, HL, HH).

7th step: Inverse DWT is applied on the sub band that result in the previous step. The resultant image of the step is called stego image

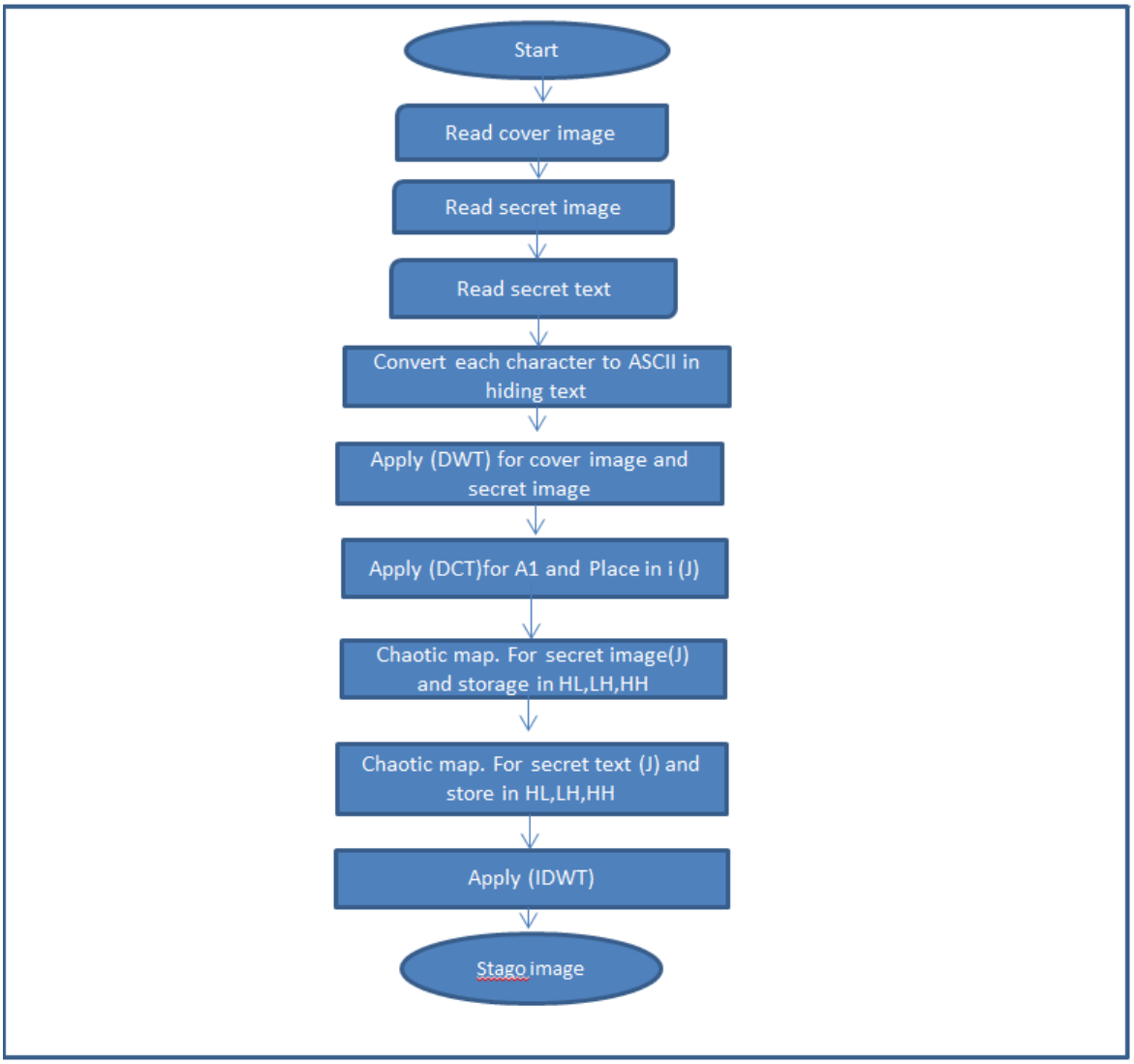

Figure (3.3) Depicting the embedding algorithm flow chart of hiding

secret image and secret text

3.3.3Extraction Process

Inputs: Stego image

Step 1: Read stego image

Step 2: Divided the stego image into layers of R, G, and B color

Step 3: Apply the (DWT) to the stego image of get to the four band (LL1,HL1,LH1,HH1)

[LL,LH,HL,HH] = dwt2(stego image,'haar');

Step 4Get three band (HL, LH, LL) which is where the text and the image are stored

Step5 : After restoring all the pixels , now we apply the inverse of the chaos

J(pixel_Order_final)=J;

J=reshape(J,[r,c]);

Step 6: Apply(IDCT)

dd = idct2(J);

Step 7: Apply the (IDWT) to get the recovered secret image and text

J=J/0.01;

dd=idwt2(dd,[ ], [],[ ],'haar');

Iextract(:,:,i)= dd;

Jtext_out=Jtext_out/0.1;

Jtext_out=Jtext_out(2:[Jtext_out(1)+2]);

Jtext_out=Jtext_out/0.1;

Jtext_out=Jtext_out(2:[Jtext_out(1)+2]);

Jtext_out(pixel_Order_final_text)=Jtext_out;

Step 8: Apply(IDCT) to the

Step 9: Apply the (IDWT) to get the recovered secret image and secret text.

Figure (3.5) depicting the extraction algorithm flow chart of extracting secret image and secret text .

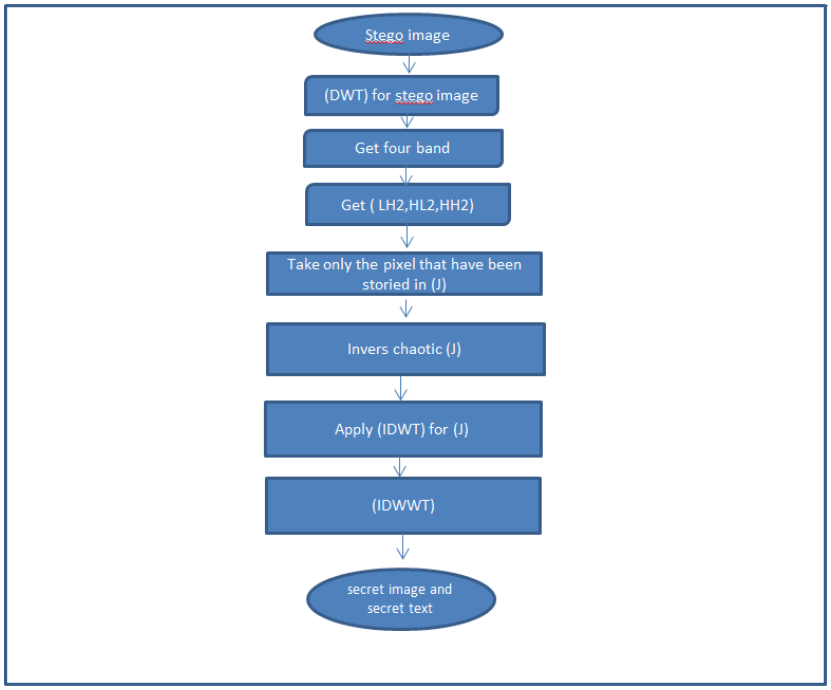

Figure (3.5) Depicting the extraction algorithm flow chart of extracting secret image and secret text.

Semulation and Results

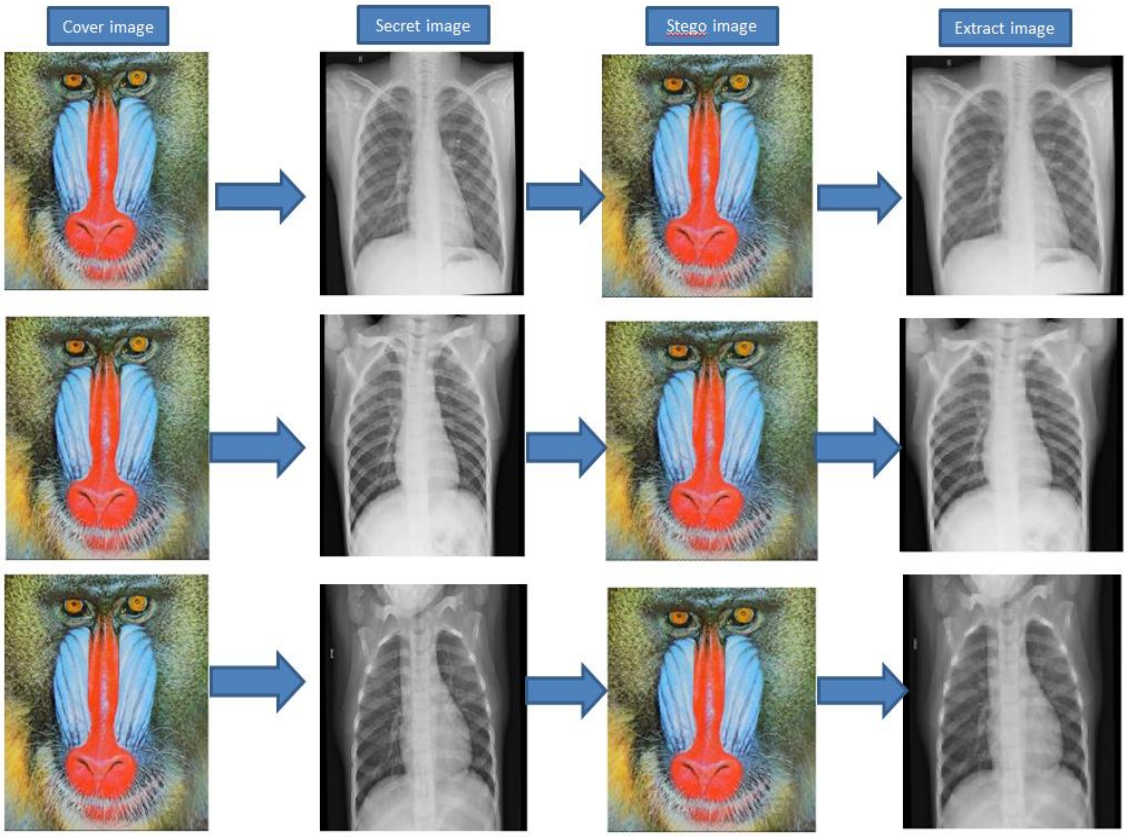

Figure (4.3) The test samples that applied to the system by method RGB

Table 4.2: Measurement of Values for 10 Images used RGB.

Image name	PSNR emb	SNR emb	MSE emb	SSIM Emb	PSNR ext	SNR ext	MSE ext	SSIM Ext
Image (1)	29.54646	24.13381	72.18296	0.955813	34.44702	28.55226	23.35492	0.935134
Image (2)	29.56084	24.14806	71.94426	0.95587	34.44449	27.48201	23.36855	0.935211
Image (3)	29.55402	24.14134	72.05742	0.955815	32.09424	25.88828	40.14728	0.928845
Image (4)	29.54647	24.13377	72.18271	0.955803	32.38084	26.69344	37.58344	0.921211
Image (5)	29.53614	24.12354	72.35459	0.955723	32.77732	28.18056	34.30432	0.929059

Image (6)	29.56267	24.1499	71.91405	0.955889	33.89977	26.73483	26.4913	0.933994
Image (7)	29.53504	24.1224	72.37295	0.955739	34.27675	29.35427	24.28874	0.93967
Image (8)	29.53062	24.11802	72.44658	0.955712	32.46899	28.37591	36.82829	0.934406
Image (9)	29.5604	24.14767	71.95155	0.955913	32.76768	25.99384	34.38049	0.928656
Image (10)	29.53754	24.12494	72.33125	0.955742	34.17234	29.79343	24.87979	0.935212

Conclusions

1. The proposed system embedded the secret image in the cover image based on Haar DWT, which provided good extracted secret image quality that led to increasing in the imperceptibility of the system.
2. Security analysis demonstrates that the proposed encryption approach has large key space, which makes a brute-force attack impracticable, because of using chaotic function to generate one-time pad.
3. Chaotic techniques successfully reduced the secret information between the sender and receiver by sending the initial conditions and control parameters. This property overcomes the key exchange problem of the encryption system. Key storage is minimal

References

[1] Johnson, N. F., Duric, Z., & Jajodia, S. (2001). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures. Kluwer Academic Publishers, USA, Vol. 1. Springer.

[2] Taqa, A., Zaidan, A. A., & Zaidan, B. B. (2009). New framework for high secure data hidden in the MPEG using AES encryption algorithm. International Journal of Computer and Electrical Engineering (IJCEE), 1(5), pp. 566-571.

[3]Katzenbisser, S. & Petitcolas, F. (2016). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House publisher, Boston, ISBN 1- 58053-035-4.

[4] Shuhui Chen, Zengqiang Chen, Zhuzhi Yuan," A Compound Video Encryption Algorithm Based on Hyperchaos", International Conference on Innovative Computing Information and Control, pp. 560, 2008.

[5] Hephzibah Kezia, Gnanou Florence Sudha, "Encryption of digital video based on lorenz chaotic system", International Conference on Advanced Computing and Communications, pp. 40-45, 2008.

[6] Nitin, K., kirit, R., Avalik, R., Vijaysinh, J. & Ashish, N. (2014). A Novel Technique for Image Steganography Techniques Based on LSB and DCT Coefficients. International Journal for Scientific Research and Development (IJSRD), 1 (11). pp. 2479-2482.

[7] Houssein , E.H.; Ali, M.A.S.; Hassanien, A.E. An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System. IEEE Proceedings of the Federated Conference on Computer Science and Information Systems.2016, 8, 641– 644, doi:

[8] Zheng Yan-bin, Ding qun," A new digital chaotic sequence generator based on Logistic Map", International Conference on Innovations in Bio-inspired Computing and Applications (IBICA), pp.175-178, 2011.

[9] Piyush Kumar Shukla, Ankur Khare, Murtaza Abbas Rizvi, Shalini Stalin, Sanjay Kumar," Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing", pp.1387-1410, Vol.17, Iss.3, 2015.

[10] Xue Wang, Lequan Min, Mei Zhang, "A Generalized Stability Theorem for Continuous Chaos Systems and design of pseudorandom number generator", International Conference on Computational Intelligence and Security, pp. 375-380, 2015