Secret image and text in image-based Chaos Theory

Doaa mahmood abass
دعاء محمود عباس
Doaamahood٤٧@gmail .com
shams dheyaa alwan
شمس ضياء علوان
shams-al-ganabi@yahoo.com

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.

proposed PSO using DWT algorithm to find optimal key that can be used to hide image with multi objective optimization. In this method, PSNR٨١,٨٧٢١ and IF can be getting., -٢,١٨٥٠e-٠٨

Both the second and third proposed methods are based on cipher , but the second method uses (RGB) and Chaotic using DWT, while the third one uses YCbCr and Chaotic using DWT . The last proposed method is implemented based SVD using DWT. can be getting PSNR successively ٢٩.٥٤٦٤٦ ,٢٩ .٣٤٩,٢٤ .٥٧٥.

For comparison, various performance indexes are measured for each method such as : PSNR,IF,MSE,SSIM

Matlab ٢٠١٨ 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 stenographic goals that are designed for this purpose.

Literature review

Below are some of the related works listed:

Shuhui Chen, Zengqiang Chen and Zhuzhi Yuan,(٢٠٠٨) 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 [١١].

Hephzibah Kezia and Gnanou Florence Sudha (٢٠٠٨) 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 ٤th 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 (٨* ٨). 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 [١٢].

Nitin, et al. (٢٠١٤)[٨] 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.

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 [٤٥].

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 [٤٦].

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 [٤٧].

Proposed method

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

٣,٣,١Embedding process

The embedding process can be applied as follows:

١st step: Divide the image into color layers (Red, Green, and Blue).

٢nd step: Apply DWT for each color of the input image and the Approximate, Horizontal, Diagonal and Vertical sub bands are obtained

٣rd step: DCT is applied for each sub band that obtained in the ٢nd step

$$DCT(I,j) = \frac{٢}{N} C(i)\, C(j) \sum_{X0}^{N-١} \sum_{Y=.}^{N-١} pixel(x,y) \quad .....(٢)$$

$$Cos\left[\frac{(٢x+١)i\pi}{٢N}\right] cos\left[\frac{(٢y+١\, j\pi)}{٢n}\right]$$

where:

• DCT (i,j) represents the value of the DCT at the point of coordinates (i, j) in the block of ٨x٨ pixels.

• Pixel (x, y) represents the value of the pixel of coordinates (x, y) in the block of the original image of ٨x٨ pixels

٤th 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

٥th step: Divide the cover image into RED, Green, Blue color layers and apply DWT for each layer.

٦th 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).

٧th 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

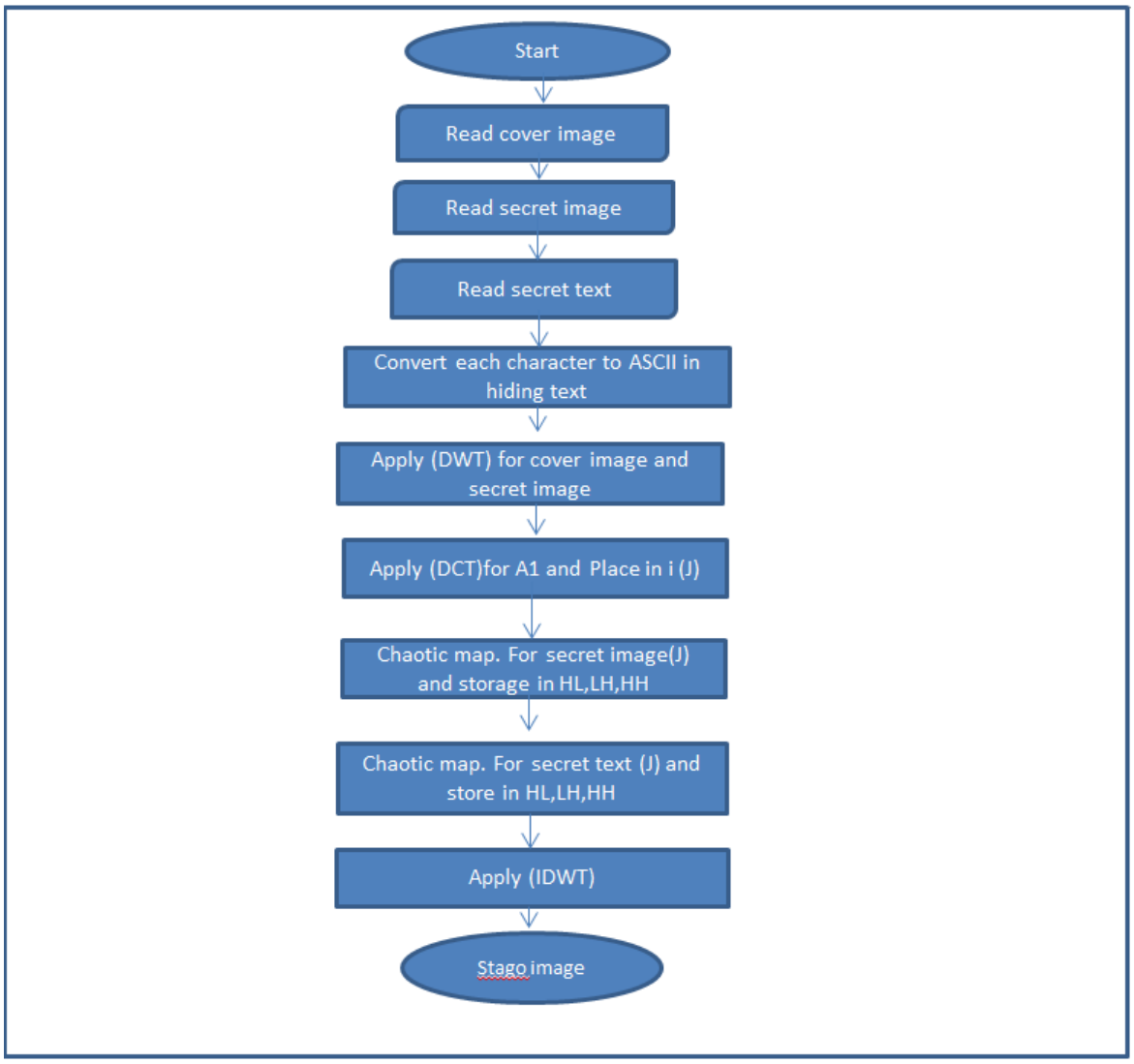

Figure (٣،٣) Depicting the embedding algorithm flow chart of hiding secret image and secret text

٣،٣،٣Extraction Process

Inputs: Stego image

Step ١: Read stego image

Step ٢: Divided the stego image into layers of R, G, and B color

Step ٣: Apply the (DWT) to the stego image of get to the four band (LL١,HL١,LH١,HH١)

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

Step ٤Get three band (HL, LH, LL) which is where the text and the image are stored

Step٥ : 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 ٧: 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 ٨: Apply(IDCT) to the

Step ٩: Apply the (IDWT) to get the recovered secret image and secret text.

Figure (٣،٥) depicting the extraction algorithm flow chart of extracting secret image and secret text .

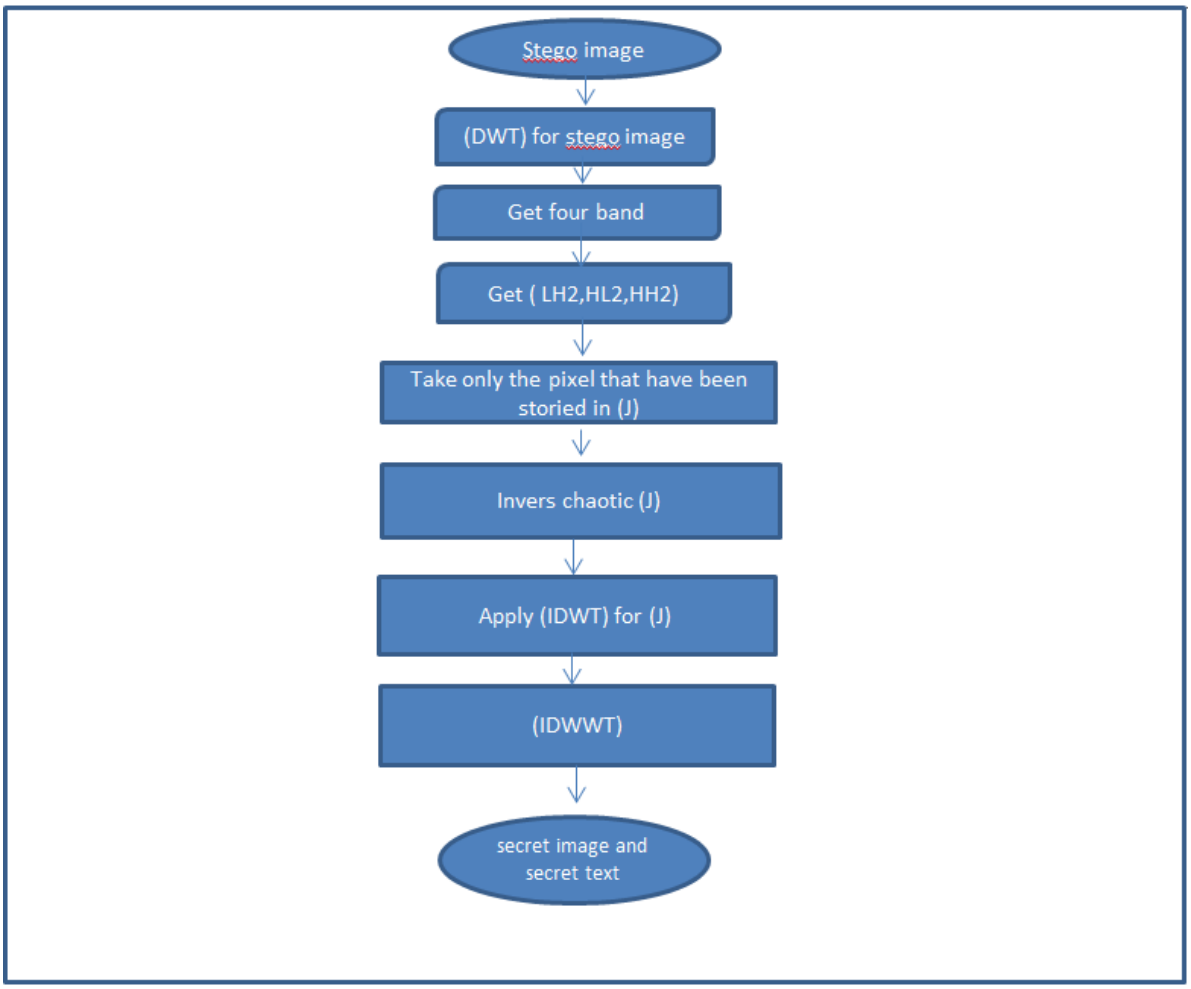

Figure (٣،٥) Depicting the extraction algorithm flow chart of extracting secret image and secret text .

Simulation and Results

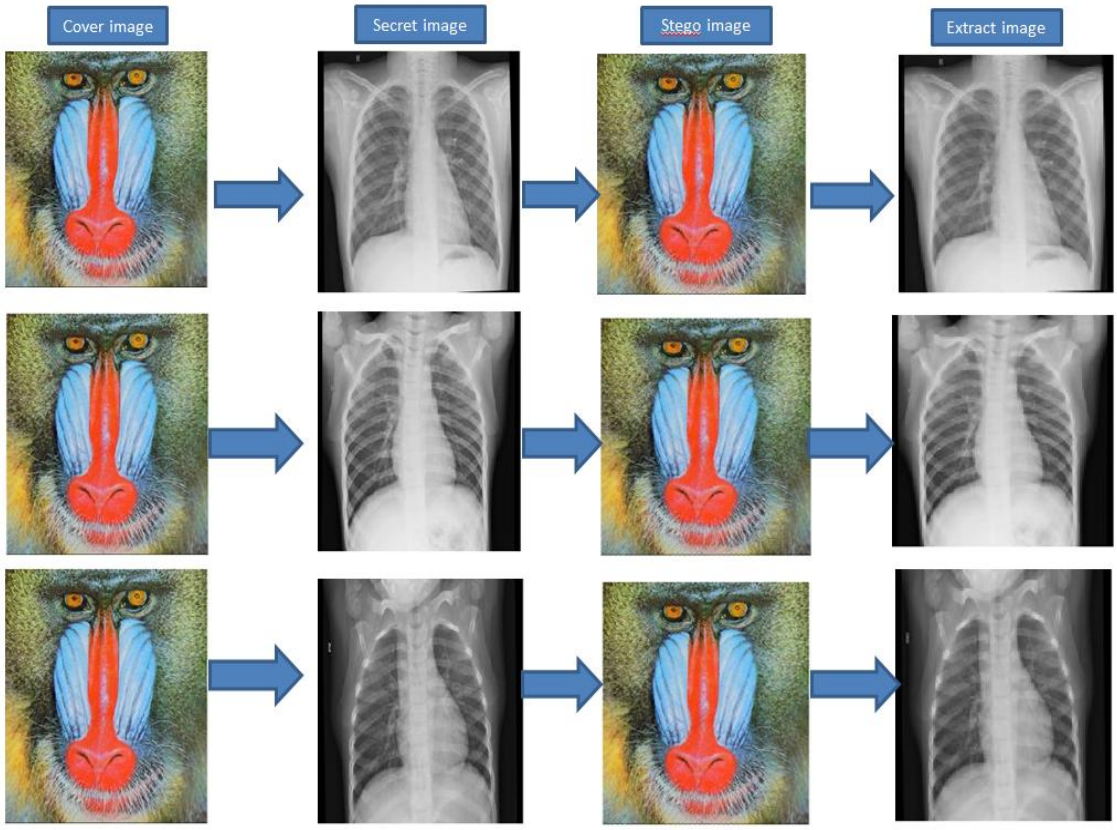

Figure (٤،٣) The test samples that applied to the system by method RGB

Table ٤،٢:Measurement of Values for ١٠ Images used RGB.

Image name	PSNR emb	SNR emb	MSE emb	SSIM emb	PSNR ext	SNR ext	MSE ext	SSIM Ext
Image (١)	٢٩.٣٥٢١٢	٢٣,٩٤٠١٨	٧٥,٤٨٦٣٧	٠,٩٥٥٠٥٥	١٠,٦٥٦٦٥	٤,٥٢٣٥١٧	٥٥٩٠,٠٥٢	٠,٧٦٥٩٥٤
Image (٢)	٢٩.٣٤٦١٧	٢٣,٩٣٤٢٣	٧٥,٥٨٩٨٤	٠,٩٥٤٩٩٥	١٩,٠٢١٦	١٢,٤٠٥٢٤	٨١٤,٥٥٤٣	٠,٨٠٣٤٥١
Image (٣)	٢٩.٣٤٤٨٩	٢٣,٩٣٢٩٨	٧٥,٦١٢١٣	٠,٩٥٤٩٨٩	١٧,١١٣٣١	١٠,٣٩٩٧٦	١٢٦٤,٠٠٧	٠,٧٧٩٠٣
Image (٤)	٢٩.٣٤٨٤	٢٣,٩٣٦٤٩	٧٥,٥٥١٠٢	٠,٩٥٥٠١٢	١٤,٩٤٩٥٨	٨,٤٦٠٣٥٤	٢٠٨٠,٢٨٢	٠,٨٤٤٠٦٧
Image (٥)	٢٩.٣٤٦٣١	٢٣,٩٣٤٣٧	٧٥,٥٨٧٤٣	٠,٩٥٥٠٠٨	١٥,٦٣٩٦٤	٩,٠٩٨٥٤٦	١٧٧٤,٦٦٥	٠,٧٦٦٨٧
Image (٦)	٢٩.٣٥١٨٨	٢٣,٩٣٩٩٨	٧٥,٤٩٠٥٣	٠,٩٥٥٠٦٣	١٧,٤٤٢٨	٩,٩٦٥٢١٣	١١٧١,٦٥٦	٠,٨٦٤٠٣٤
Image (٧)	٢٩.٣٥٠٥٧	٢٣,٩٣٨٦٨	٧٥,٥١٣٢٤	٠,٩٥٥٠٣١	١٥,٤٣٢٩٤	٨,٥٣٧٠١٣	١٨٦١,١٧٣	٠,٧٧٦٨٠٣
Image (٨)	٢٩.٣٤٤٣	٢٣,٩٣٢٤٢	٧٥,٦٢٢٣	٠,٩٥٤٩٨٢	٢٠,٠٦٢٧١	١٢,٧٩٦٥٥	٦٤٠,٩٢٧٨	٠,٩١٦٧٨٤

Image (٩)	٢٩.٣٤٩٢٤	٢٣,٩٣٧٤	٧٥,٥٣٦٤٣	٠,٩٥٥٠٠٦	١٢,٨٠٥٥١	٦,١٣٥٢٤٥	٣٤٠٨,٢٣	٠,٧٩٢٢٧٢
Image (١٠)	٢٩.٣٤٥٤٢	٢٣,٩٣٣٤٧	٧٥,٦٠٢٩٢	٠,٩٥٤٩٨٨	٢٠,٨٩٥٧٦	١٣,٥٧٥٥٧	٥٢٩,٠٥٩١	٠,٨٤١٣٣
Image (١١)	٢٩.٣٤٧٢٩	٢٣,٩٣٥٤	٧٥,٥٧٠٣١	٠,٩٥٥٠٠٩	١٣,٧٣٣٥٦	٦,٦٣٨٦٤٧	٢٧٥٢,٤٨	٠,٧١٢٢٣٢
Image (١٢)	٢٩.٣٥١٥٣	٢٣,٩٣٩٥٣	٧٥,٤٩٦٥١	٠,٩٥٥٠٣	١٥,٢٣٥١٥	٨,٧١١٠٠٧	١٩٤٧,٨٩٣	٠,٨٣٦٦٠١
Image (١٣)	٢٩.٣٤٨٧٧	٢٣,٩٣٦٨٧	٧٥,٥٤٤٦٦	٠,٩٥٥٠٣٢	١٤,١٩٢٢٢	٧,٧٣٥٩٤٢	٢٤٧٦,٦١٦	٠,٧٧٨٤٦١
Image (١٤)	٢٩.٣٤٩١٥	٢٣,٩٣٧٢٨	٧٥,٥٣٧٩٢	٠,٩٥٥٠٣٣	١٤,٩٨٤٠٥	٨,١٠٥٧٢٦	٢٠٦٣,٨٣٧	٠,٨٤٥٦٤٤
Image (١٥)	٢٩.٣٤٠٨٤	٢٣,٩٢٨٨٨	٧٥,٦٨٢٧٤	٠,٩٥٤٩٤٦	٢٤,٤١٧٨٩	١٦,٤٢٦٢٤	٢٣٥,١٢٠٨	٠,٨٦١٤٢٦
Image (١٦)	٢٩.٣٤٧٢٥	٢٣,٩٣٥٤٤	٧٥,٥٧١٠٣	٠,٩٥٥٠٠٨	١٦,٦٤٥٠٢	٩,٧٣٠٠٩٤	١٤٠٧,٩٢١	٠,٨٥٣٠٢١
Image (١٧)	٢٩.٣٤٦٤٢	٢٣,٩٣٤٤٥	٧٥,٥٨٥٤١	٠,٩٥٥٠٠٩	١٦,٨٨٥٣٩	١٠,٠٢٦٥٦	١٣٣٢,١١٣	٠,٧٧٢٣٥٧
Image (١٨)	٢٩.٣٤٧١٣	٢٣,٩٣٥١٩	٧٥,٥٧٣١	٠,٩٥٥٠١٤	١٤,٩٣١٤٥	٨,٣١٦٧١٢	٢٠٨٨,٩٨٥	٠,٧٩٨٥٥٥
Image (١٩)	٢٩.٣٤٨١٤	٢٣,٩٣٦١٧	٧٥,٥٥٥٤٨	٠,٩٥٥٠٢٦	١٢,٨٢٥٩٢	٥,٨٩٠٢٥	٣٣٩٢,٢٥١	٠,٨١٧٧
Image (٢٠)	٢٩.٣٥٤٩٣	٢٣,٩٤٣٠٣	٧٥,٤٣٧٥٣	٠,٩٥٥٠٩٥	١٤,٨٧١١٨	٧,٥٩٨٤٢٨	٢١١٨,١٧٦	٠,٧٨٧٥٥٨
Image (٢١)	٢٩.٣٤٥٥٢	٢٣,٩٣٣٥٧	٧٥,٦٠١٢١	٠,٩٥٤٩٨	١٦,٨٠٣٩٥	٩,٩٢١٤٨٩	١٣٥٧,٣٣١	٠,٨١٨٧٧٧
Image (٢٢)	٢٩.٣٤٧٠٨	٢٣,٩٣٥٢	٧٥,٥٧٣٩٦	٠,٩٥٤٩٩٧	٢٠,٧٠٩١٤	١٣,٣٩٨١٧	٥٥٢,٢٨٩٣	٠,٨٢٦٦٢٣
Image (٢٣)	٢٩.٣٤٢٦٨	٢٣,٩٣٠٧٨	٧٥,٦٥٠٦٧	٠,٩٥٤٩٤٨	٢٥,٧٠٨١١	١٧,١٤٥٠٩	١٧٤,٦٩٠٧	٠,٩٤٠٨٩٧
Image (٢٤)	٢٩.٣٤٦٥	٢٣,٩٣٤٦٧	٧٥,٥٨٤٠١	٠,٩٥٥٠١١	١٩,٩٤٣٢٢	١٢,٨٣٩٠٦	٦٥٨,٨٠٦٧	٠,٨٤٦٨٦٧
Image (٢٥)	٢٩.٣٤٥٦٧	٢٣,٩٣٣٧٦	٧٥,٥٩٨٥٥	٠,٩٥٥٠١٣	١٣,٢٣٧٦٦	٦,٣١٥٦٥٣	٣٠٨٥,٤٢٤	٠,٧١١١١٦
Image (٢٦)	٢٩.٣٤٦٢	٢٣,٩٣٤٢٥	٧٥,٥٨٩٢٥	٠,٩٥٤٩٩٨	١٥,٦٤١٠٢	٩,٠٦٧٩١٢	١٧٧٤,١٠١	٠,٨٠٣٠٠١
Image (٢٧)	٢٩.٣٤٧١٨	٢٣,٩٣٥٣١	٧٥,٥٧٢٢٢	٠,٩٥٤٩٩٦	٣٠,٨٦٨٣٤	٣٠,٨٦٨٣٤	٥٣,٢٤١٠٧	٠,٩٢١٩٤٨
Image (٢٨)	٢٩.٣٤٦٨٣	٢٣,٩٣٤٩٣	٧٥,٥٧٨٤٢	٠,٩٥٥٠٠٨	٢٤,٢٧٤٣٩	١٦,٦٢٦٩٨	٢٤٣,٠١٩٦	٠,٨٥٨٨٥٢
Image (٢٩)	٢٩.٣٤٧٦٢	٢٣,٩٣٥٧٣	٧٥,٥٦٤٥٣	٠,٩٥٥٠٠٧	٢٩,٨٤٦٣	٢١,٧٩٥٥	٦٧,٣٦٧٤٦	٠,٩٠٤٦٧٨
Image (٣٠)	٢٩.٣٤٧٠١	٢٣,٩٣٥١١	٧٥,٥٧٥٢٢	٠,٩٥٥٠١٥	١٥,١٧٣٠١	٨,٨٤٧٦٣٨	١٩٧٥,٩٦٦	٠,٧٩٧٢٩١

Conclusions

١. 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.

٢. 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.

References

[١] Johnson, N. F., Duric, Z., & Jajodia, S. (٢٠٠١). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures. Kluwer Academic Publishers, USA, Vol. ١. Springer.

[٢]Taqa, A., Zaidan, A. A., & Zaidan, B. B. (٢٠٠٩). New framework for high secure data hidden in the MPEG using AES encryption algorithm. International Journal of Computer and Electrical Engineering (IJCEE), ١(٥), pp. ٥٦٦-٥٧١.

[٣]Katzenbisser, S. & Petitcolas, F. (٢٠١٦). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House publisher, Boston, ISBN ١-٥٨٠٥٣-٠٣٥-٤.

[٤] Shuhui Chen, Zengqiang Chen, Zhuzhi Yuan," A Compound Video Encryption Algorithm Based on Hyperchaos", International Conference on Innovative Computing Information and Control, pp. ٥٦٠, ٢٠٠٨.

[٥] Hephzibah Kezia, Gnanou Florence Sudha, "Encryption of digital video based on lorenz chaotic system", International Conference on Advanced Computing and Communications, pp. ٤٠-٤٥, ٢٠٠٨.

[٦]Nitin, K., kirit, R., Avalik, R., Vijaysinh, J. & Ashish, N. (٢٠١٤). A Novel Technique for Image Steganography Techniques Based on LSB and DCT Coefficients. International Journal for Scientific Research and Development (IJSRD), ١ (١١). pp. ٢٤٧٩-٢٤٨٢.

[٧] 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.٢٠١٦, ٨, ٦٤١– ٦٤٤, doi:

[٨] 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.١٧٥-١٧٨, ٢٠١١.

[٩] 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.١٣٨٧-١٤١٠, Vol.١٧, Iss.٣, ٢٠١٥.

[١٠]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. ٣٧٥-٣٨٠, ٢٠١٥