IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Chaotic Based Image Cryptography Using Wavelet Transform

[1] Dr P Shanthi
[1] Assistant Professor, Department of Information Technology, VHNSN College (Autonomous),Virudhunagar, TamilNadu, India.

Abstract - **The main objective of the paper is to enhance the security of the images using chaotic map with wavelet transform. Chaos-based image encryption method is one of the most efficient methods which is used to hide visual information during transmission. This paper presents a new image encryption method based on Arnold cat map with Wavelet Transform, in which, chaotic maps will change the pixels of the plain-image to encrypt that. Finally, the encrypted image will be decrypted to remake the plain-image. To evaluate the efficiency of this method, it has been implemented with MATLAB and also has been measured by doing some tests as analysis of Peak signal-to-noise ratio and adding salt & pepper noise. Simulation results shows that the proposed image encryption method has high accuracy while it is resistant against salt & pepper noise**

Keywords: Iimage encryption, chaotic maps, Arnold Cat map and Wavelet Transform.

I. INTRODUCTION

The main aim of cryptography is hiding the data or message from the intruders. In medical and military fields, images are transferred in encrypted forms due to security reasons. It will be sent only to the intended users; hence intruders cannot view the image. Hence Images are encrypted with several methods, and it will be shared with the receivers. Receiver will reverse the same process and get the original image. But in the above process, it is possible that intruders may access the encryption technology, hence unauthorized may access the image. Hence, a new technology is implemented in the proposed system. A secret key will be generated using a password which assigned during encryption, based on the key, image will be encrypted. Arnold cat map is used to shuffle the pixel position .The wavelet Transform is used for encryption process. Any of the above wavelet will be chosen for encryption based on the key generated at the initial step. Secret password and the encrypted image will be shared with the intended receiver. Hence the receiver can decrypt the image using same key. After applying the key, same wavelet which is used for encryption will be selected and applied to the encrypted image. The whole process will be reversed and original image will be retrieved.

A chaos based image encoding algorithm, where the pixels of the image will be repositioned and the relation between original and encoded image will be collapsed8. A cipher technology, where an external key will be used to perform chaotic operation to remove the relationship between original image and encoded image. An encryption scheme, in which Discrete Cosine Transform (DCT) applied to the intended image, lowest frequency of the particular image will be used a key for encryption. Hence, data loss will be lesser when compared with other encryption schemes. Similarly, Discrete Cosine Transform (DCT) applied to the targeted image and used highest frequency co-efficient to encrypt the image [2006]. Haar Wavelets are used to decompose the image and positions of pixels are rearranged to ensure the security of image. Hence, the human visibility will remain in the encoded image. Some researchers are using image based transform to encrypt the images [2010]. The most common method for encrypting the image is 2-D Haar wavelet transform [2012]. 2-D wavelet transform will be applied to the image, resulted frequency sub bands will be shuffled and repositioned in different ways. On the contrast whole process will be reversed for retrieving the original image. In this paper, Choatic maps and Wavelet transform is chosen for encryption process. Discrete Wavelet transform provides more information and higher flexibility for processing the image. Data of images will be retrieved exactly rather than other block based transformations.

II. LITERATUR REVIEW

Chaos is a phenomenon that occurs in deterministic non-linear systems that has high sensitivity to the initial condition and shows a pseudo random behavior at the same of being deterministic. It means that by having initial values and mapping function, we can regenerate the exact initial values. Small change in initial condition will cause a great change in the future. This phenomenon in chaos theory is called Butterfly effect. Such systems will stay in chaos mode so that can have the condition of Lyapunov exponential equation. An important feature that makes this phenomenon being highly regarded for encryption is the definability of the system and at same time having the pseudo random behavior that causes the output of the system seems randomly at attacker's point of view, while it is definable at a decoder of Cipher system point of view so it can be decrypted easily.

In [2014] Shanthi et al proposed robust chaos based image watermarking scheme for Fractal Wavelet.In this paper Arnold cat Map and logistc maps are used to do image watermarking in a high security manner. Haar wavelet transform is used in dual image watermarking using DWT-SVD in [2015].Chaotic maps with SVD used in Dual Image watermarking in [2016].

Many encryption algorithms base on chaos are proposed. Pareek and Patidar (2006) have proposed a new way of image encryption scheme which utilizes two chaotic logistic maps and an external key of 80-bit. The initial conditions for both the logistic maps were derived using the external secret key by providing weightage to its bits corresponding to their position in the key. Gao and Chen (2006) presented an image encryption scheme which employs a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image.

III. BACKGROUND

A Arnold Cat Map

One of the most important chaotic functions is cyclic chaoticfunction that each time applied on a square image rearranges its pixels. In order to shuffle the embedding position of the host image, two dimensional Arnold cat map is employed in this scheme. After that logistic map is applied to find an embedding position. The generalized form of Arnold's cat map can be given by the transformation

$\Gamma : T2 \rightarrow T2$

such that:

$x' = x+y$

$y' = x+2y$

Where $x, y \in \{0, 1, 2 \ldots n-1\}$ and n is the size of a digital image.

Let p be the transform period of an $N \times N$ digital image I. Applying ACM for a random iteration of t times ($t \in [1, p]$) to I, a scrambled image I` is obtained which is completely chaotic and different from I. Now I` can be transmitted over the communication channel without revealing any information to the unauthorized receivers. At the receiving end, the process is repeated for ($p - t$) times to obtain back the original image.

B .DISCRETE WAVELET TRANSFORM

Wavelet transform represents a valid alternative to the cosine transform. Discrete Wavelet transform is a multi-resolution decomposition of a signal. The DWT of images is a transform based on the tree structure with D levels that can be implemented by using an appropriate bank of filters. Essentially, it is possible to follow two strategies that differ from each other basically because of the criterion used to extract strings of image samples to be elaborated by the bank of filters.

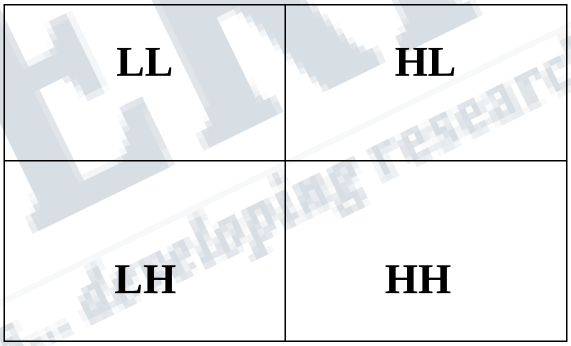


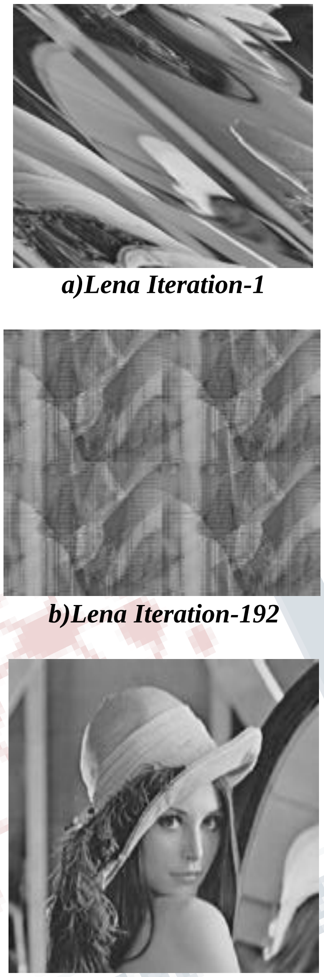
Figure 1. Frequency Sub bands after applying wavelet transform to an image

IV. PROPOSED IMAGE ENCRYPTION ALGORITHM

A Encryption Algorithm

At the first step, Password will be created for encrypting the image. Text or special characters of the password will be used by the key generating algorithm a secret key will be generated. This generated key will not even known to the sender. Based on the key, encryption process will be carried out.

At first, Arnold Cat Map is applied to the host image. In this paper ACM is applied T times to the host image where, T is the period of the chaotic function of the image is calculated as depending on image size. The ACM is applied (T/2) times to the host image for creating the chaotic image with best distribution .As an example, the standard test image Lena is considered with pixel size 512×512 where, T = 384.In Figure 2 shows the images for first ,192 and 384 iteration of ACM.LM is applied to (T/2) times iteration of the host and get the scrambling of an image.



a)Lena Iteration-1

b)Lena Iteration-192

c)Lena Iteration-384

Figure 2. Process of Arnold cat map on Lena Image

Then the wavelet transform will be chosen from the wavelet choosing function in the algorithm.. First level of wavelets produces four sub band matrix for the given image. LL -> low-low frequency sub band, LH-> low-high frequency sub band, HL-> high-low frequency sub band, HH-> high-high frequency sub band. Next step is decreasing the values of low-low frequency sub band by LL(i,j)->LL(i,j)/(m×n), where m and n are the dimensions of the low-low frequency sub band. Next step will be reversing the signs of LH, HL and HH sub bands, to inverse the magnitude of sinusoidal co-efficient.

It will make brighter side to darker and darker side to brighter. Next two steps are the important process of this paper. Positions of the sub bands will be exchanged through three patterns,

1. Exchanging LL with HL and HL with LL
2. Exchanging LL with LH and HL with HH.
3. Exchanging LL with HH and LH with HL.

Based on the key, any one of the pattern will be chosen for exchanging the positions of sub bands. This process will be carried in two steps, at first step, a pattern will be applied and in the second step, another pattern will be chosen for exchanging the positions of sub bands. Figure 3 explains the process of choosing wavelet mechanism and exchange of frequency sub bands. Now the Inverse Discrete Wavelet Transform (DWT) will be applied to produce the encrypted image. Thus the encrypted image and password will be shared only with the intended receiver.

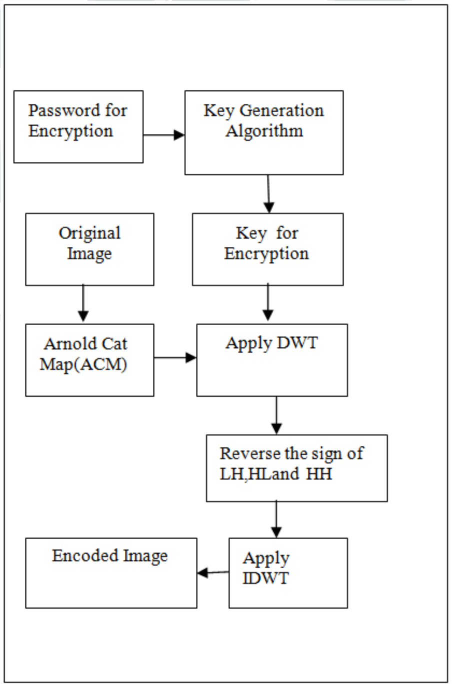


Figure 3 Encryption Process

B Key Generation Algorithm

For generating the key, Password given by the sender will be passed to the algorithm initially.

STEP 1:

Number of elements in the password will be calculated and based on the numbers, modulo will be taken to all characters, thus the number produced will be assigned as key.

STEP 2:

Three values of the key will be chosen and they are assigned to different tasks such as Wavelet Identifier, First Level Sub band Exchanger and Second Level Sub band Exchanger.

STEP 3: First key value will be passed to the wavelet selection mechanism, based on the value derived from the key, a wavelet will be chosen.

STEP 4: Second key value, which will be used for selecting the pattern for exchanging the sub band matrix positions.

STEP 5: Third key value, which will be used for selecting second level of exchanging patterns in the already exchanged sub band matrix.

C Decryption Algorithm

In the decryption algorithm, whole process will be reversed to generate the original image. Receiver will be prompted to enter the password for generating the decrypted image.

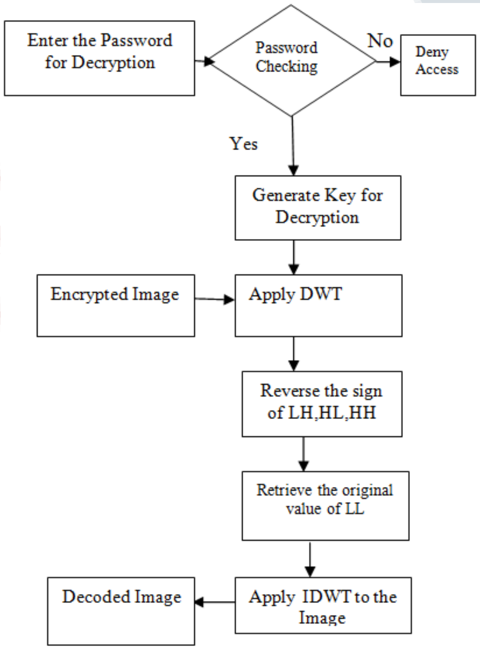

Enter the Password for Decryption
Password Checking
No
Deny Access
Yes
Generate Key for Decryption
Encrypted Image
Apply DWT
Reverse the sign of LH,HL,HH
Retrieve the original value of LL
Decoded Image
Apply IDWT to the Image

Figure 4 Decryption Process

If the password is same given by the sender, receiver will be allowed to decrypt the image, otherwise decryption process will be terminated. Similarly a key will be generated from the given password, hence, wavelets will be chosen to apply Discrete Wavelet Transform (DWT).

First step of the decryption will be second level of exchanging the sub band. Second step is exchanging the sub band as in the first level of encryption process. Now the values of LH, HL and HH will be inversed by multiplying (-1). During Encryption process, values of LL were lessened, now the same values will be recreated through LL(i,j)->LL(i,j)×(m×n). Figure 4 shows the decryption process. Thus at the final step, inverse wavelet transform will be applied to bring back the original image.

V. EXPERIMENTAL ANALYSIS

Different images in different sizes were used for experimental analysis; the above algorithm fits to all test images carried out. PSNR (Peak Signal Noise Ratio) is the main test conducted to verify the originality of the received image. If the resultant value of PSNR is 30db or greater, then there will not be a difference between original and decrypted image. In the proposed algorithm PSNR value lies between 35db and 40 db. Figure 5 explains the Encryption and decryption process, At the left Original Lena and Boat images are shown, Encrypted images of Lena and Boat images are shown in the center, Decrypted images of Lena and Boat images are shown at the right. Hence, there will be a small distortion in a decrypted image. Similarly Figure 5,6 and 7 shows the same result using the proposed encryption and decryption process. Therefore, intruders cannot trace the logic behind encryption and decryption involved in the proposed algorithm. Table 1 shows the comparison of PSNR values between encrypted and decrypted images.

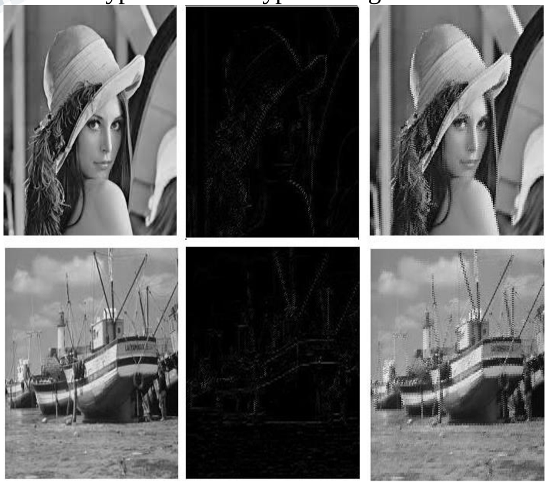


Figure 5. From top to bottom, standard test images Lena and Boat, from right to left, the figure presets the Original, Encrypted and Decrypted algorithm results.

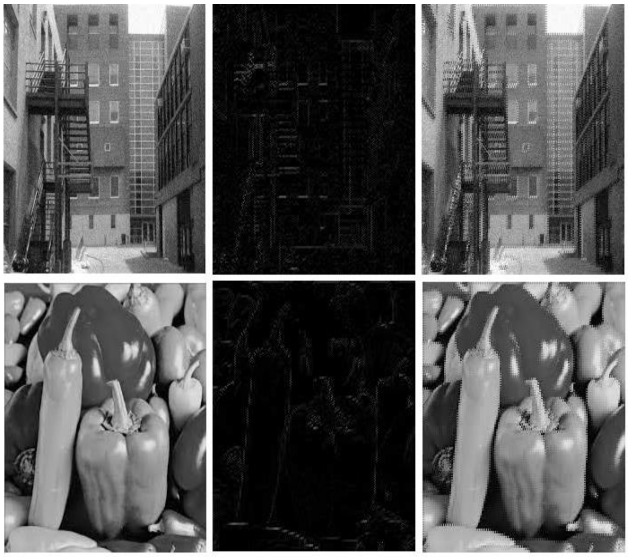


Figure 6. From top to bottom, standard test images Building and Pepper, from right to left, the figure presets the Original, Encrypted and Decrypted algorithm results.

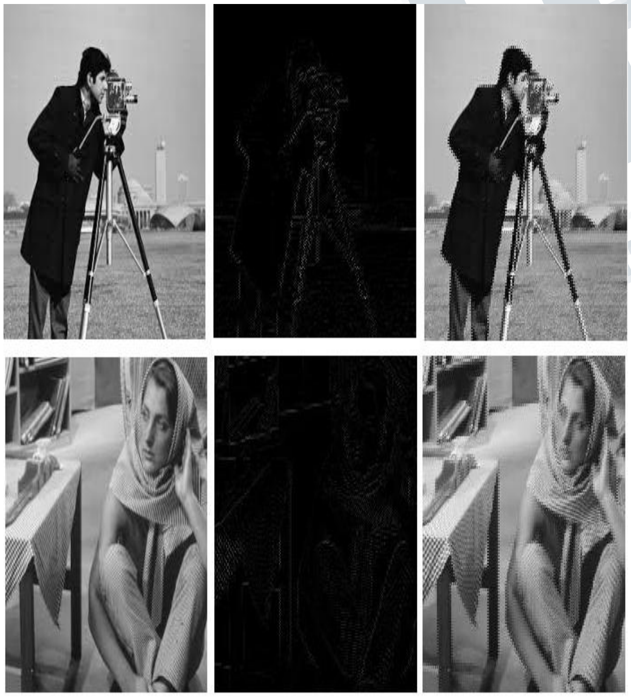


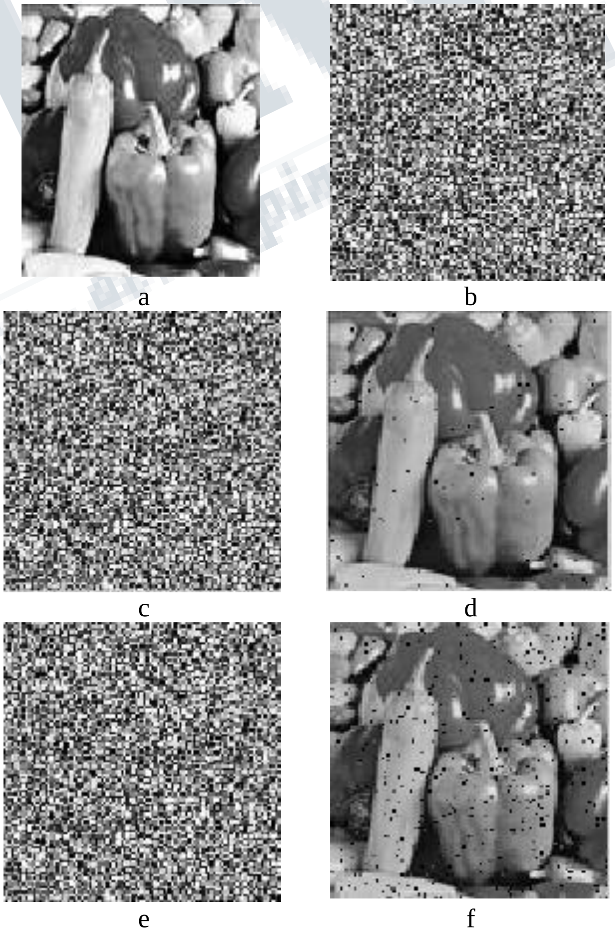
Figure 7. From top to bottom, standard test image Cameraman and Barbara, from right to left, the figure presets the Original, Encrypted and Decrypted algorithm results.

VI. SECURITY ANALYSIS

In our proposed work, symmetric key is used for both encryption and decryption. Key will be generated separately by the sender using a password. Same password will be shared with the receiver to decrypt the image. Values of generated keys cannot be determined by the hackers without knowing the algorithm used for creating the keys. Computations of key generation also very less, hence it will not cause additional overhead to the system. The security analysis can be done by two metrics. They are Salt and Pepper Noise and Peak signal Noise ratio(PSNR).

A. Adding Salt & Pepper noise

In this section, first we transmuted the plain-image to encrypted form and then added Salt & Pepper noise with different noise rate. At least we decrypted the images. Results of simulation are shown in Fig. 8.



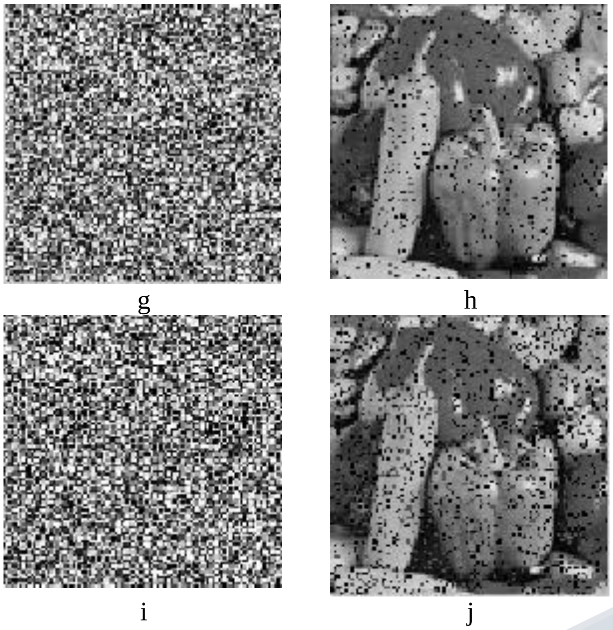


Fig 8. (a) plain-image, (b) encrypted image before applying Salt & Pepper noise, (c) the encrypted image added with 1% Salt & Pepper noise, (d) the decrypted image of (c), (e) the encrypted image added with 5% Salt & Pepper noise, (f) the decrypted image of (e), (g) the encrypted image added with 10% Salt & Pepper noise, (h) the decrypted image of (g), (i) the encrypted image added with 20% Salt & Pepper noise, (j) the decrypted image of (i). (Applying Salt & Pepper noise)

B. Peak Signal to Noise Ratio(PSNR)

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between the attacked image and the original image. The PSNR formula is defined as follows:

$$PSNR = log_{10} \frac{255 * 255}{\frac{1}{H * W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [\,[f(x,y) - g(x,y)]]^2}$$

Table 1. Results of PSNR test with various standard images and decrypted images

Standard Test Images	PSNR Values
Lena	39.02
Peppers	36.23
Building	37.04
Boat	36.45
Cameraman	38.32
Barbara	38.85

Table 1 shows the various standard test images with their PSNR Values.

VII. CONCLUSION

Many algorithm proposed under frequency domain of an image, similarly in this paper, frequency domain is used for encrypting the image. The frequency sub bands plays a vital role in encryption part of this algorithm, positions of frequency band will be rearranged in a random man¬ner, which cannot led to any guess for intruders. Arnold cat map is used to increase the security level of Image cryptography. Hence the security of the image is bolted in this paper. Various security measures have been carried out to analysis the efficiency of the algorithm and the results of the test shows the robustness of the algorithm. Algorithm com¬pared with many different benchmark algorithms and hence the proposed work shown the expected result.

REFERENCES

[1] P.Shanthi, R.S Bhuvaneswaran "Robust Chaos Based Image watermarking Scheme For Fractal-Wavelet" is published in Applied Mathematical Sciences Vol. 8 No.32,1593-1604 (2014).

[2] T. Gao, Z. Chen, "Image encryption based on a new total shuffling algorithm," Chaos, Solitons and Fractals 38, pp. 213–22,2006.

[3]P.Shanthi, R.S Bhuvaneswaran "Dual Image Watermarking using DWT and Choatic Maps" is published in International Journal of Applied Engineering Research Vol.10 No.31 (2015).

[4] N.K. Pareek, V. Patidar, K.K. Sud, "Image Encryption using chaotic logistic map," Image and Vision Computing 24, pp.926-934, 2006.

[5]Ismail IA, Amin M, Diab H. A digital image encryption algorithm based a composition of two chaotic logistic maps. IJ Network Security. 2010;11(1):1–10.

[6]Tedmori S, Al-Najdawi N. Lossless image cryptography algorithm based on discrete cosine transform. Int Arab J of Technol. 2012; 9(5):471–8.

[7]. Van Droogenbroeck M, Benedett R, editors. Techniques for a selective encryption of uncompressed and compressed images. Advanced Concepts for

Intelligent Vision Systems (ACIVS). 2002 Sep 9-11: Ghent, Belgium.

[8]P.Shanthi, R.S Bhuvaneswaran "Dual Image Watermarking Based on DWT-SVD " is published an "International Journal of Future Innovative Science and Engineering Research (IJFISER) " Volume-2, Issue-4, Dec - 2016.