International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5779
***Article Received**: 24 August 2022 **Revised**: 04 October 2022 **Accepted**: 19 October 2022*

Discrete Wavelet Transform based Cryptosystem

Soumya Babu H (Author)[1], Dr. Vijayakumar N[2], Dr. Gopakumar. K[3]
[1]Research Scholar
College of Engineering Trivandrum
Trivandrum, India
e-mail: soumiyam@gmail.com
[2]Principal (Retd.)
Govt. Engineering College, Barton Hill
Trivandrum, India
mail: dr.nvkr@gmail.com
[3]IQAC Coordinator,
APJ Abdul Kalam Technological University
Trivandrum, India
mail: gopan10dec@gmail.com

Abstract—In this article, the authors proposed, implemented and analysed a symmetric key cryptographic algorithm that can be considered as a lossless encryption and decryption technique, advantageous especially in situations where, even a slight marginal distortion is not tolerable. In the proposed system, Haar wavelet is used initially, to transform the original target image into its frequency domain, followed by encrypting the resulting sub-bands, so as to obtain a secure and reliable encrypted image. The resulting coefficients after Haar decomposition is scattered using a reversible weighing factor, suitably reversed and swapped to get the secure encrypted image. The encrypted image is then correspondingly decrypted, by the reverse process to get back the original decrypted image. Statistical testing and security methods were used to evaluate and analyse the proposed cryptosystem and the results showed that the proposed system is cryptographically resistant to attacks and is also highly secure when compared to other cryptographic systems in the frequency domain.

Keywords- DWT; IDWT; encryption; Lossless Image Encryption; symmetric key encryption; decryption; statistical testing**.**

I. INTRODUCTION

Cryptography is a method of data transmission and storage by which the data is encrypted in a manner, that can be processed only by the targeted subject. Cryptography thus, provides an efficient way to either transmit data over unsecured routes or to securely store sensitive and secret data [1][2].Cryptography can be used to encrypt different types of data such as images, text, audio messages etc [3]. Encryption of images can be either lossy or lossless, and the choice is made, depending upon the type of the application. In applications requiring highly classified images and also in satellite images, medical images etc, there is a need for original images that are distortion–free and hence uses lossless encryption methods to encrypt. In applications where decrypted images with little distortion from the original images are acceptable, lossy encryption is applicable.

The proposed cryptosystem is based on three processes, the visual and value transformation and position permutation [4]. Here, Discrete Wavelet Transform (DWT) is used to transform the original image into frequency domain with two levels of decomposition and the resulting sub-bands are modified in such a way that, it cannot be transformed back to its original form without the use of proper decryption process.

The article is organized as follows: Literature review of previous works and the significance of the current work are presented in section 2. Section 3 discusses the proposed encryption and decryption algorithm by using the application of DWT to obtain the sub-bands at two-levels of decomposition. The analysis and experimental results are discussed in section 4 and the conclusion of the research is presented in section 5.

II. RELATED WORKS

The image encryption schemes can be broadly classified into two types: frequency domain and spatial domain. Spatial domain, deals with the direct manipulation of image pixels in the image plane itself. These approaches makes the encrypted images incompressible by destroying the correlation between the pixels in the image. In frequency based approach, the frequencies of an image are modified to perform the encryption. Further, the image pixels can be totally recovered back with an inverse method with very less information loss [5]. Thus, a combination of both methods can result in enhanced security for the proposed system. The frequency based encryption can be either image based or block based. In block based system, Discrete Cosine Transform or DCT is used for encryption but can lead to blocking artefacts that

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5779
***Article Received**: 24 August 2022 **Revised**: 04 October 2022 **Accepted**: 19 October 2022*

inturn affect the image reconstructed. Also, DCT doesn't work efficiently with binary images with low spatial frequencies followed with small but sharp transitions. To overcome this issue, wavelet functions can be used, which allows a better localization in both time domain and frequency domain. Many efforts were made In 2012, a novel method of image encryption using multi level wavelet transform supported by compression was proposed by C. Samson & V. Sastry, in which a compressed image is obtained by first decomposing the image using 2-D wavelet transform followed by thresholding [6]. In 2009, C. Pang proposed an image encryption system that is based on 2-D cat mapping and DWT [7]. Krikor et al. in 2009, proposed an Image encryption method of using DCT and stream cipher which works by selecting DCT high frequencies as the characteristic values. The resulting encrypted blocks are then shuffled using a PRBS is later used to shuffle the encrypted blocks [8]. S.Tedmori and N.Al-Najdawi in 2014 later proposed an Image Cryptographic system based on the Haar Wavelet Transform by converting the original image into frequency domain followed by the reversing and shuffling of frequency subbands [9].

III. PROPOSED ALGORITHM

A. Proposed Encryption Algorithm

In the proposed encryption algorithm, two levels of wavelet decompositions are performed on the target image to be encrypted. Discrete Wavelet Transform (DWT) is used to compute the wavelet decomposition of the target image to obtain the approximation coefficients matrix A_1 and details coefficient matrices H_1, V_1 and D_1 using the Haar transform.

Haar wavelet proposed by Alfréd Haar in the year 1909 represents a sequence of square-shaped functions together forming a wavelet basis. For an input represented by a list of 2n numbers, the transform pairs the input values, storing the difference and passing the sum. The process is repeated, pairing up the sums finally resulting in 2^n- 1 differences and one sum. Haar wavelet's transform can be expressed in matrix form $H = ACA^T$ where C is an N x N matrix, A is an N x N Haar transformation matrix, and H is the resulting N x N transform that contains the Haar basis functions, $a_k(Z)$, which are defined over the interval $Z \in [0, 1]$ for k = 0, 1, 2, ... , N - 1, where $N = 2^n$.

The Haar basis functions are represented by equations (1) and (2)

$$a_0(Z) = a_{00}(z) = 1 / \sqrt{N}, \quad Z \in [0,1] \tag{1}$$

$$a_0(Z) = a_{ij}(Z) = \frac{1}{\sqrt{N}} \begin{cases} 2^{\frac{i}{2}} & , (j-1) / 2^i \le z < (1-0.5)/2^i \\ -2^{\frac{i}{2}} & , \quad (j-0.5) / 2^i \le z < / 2^i \\ 0. & otherwise \end{cases} \tag{2}$$

The size of the approximation coefficient A_1 is used as the encryption key to eliminate or diminish the A_1 values. Next step involved is the reversal of the remaining detail coefficients by multiplying each of the coefficients with (-1). It corresponds to contrast-reversal, ie, the dark changes to bright and bright changes to dark. It is followed by the swapping of the contents of A_1 with V_1 and H_1 with D_1. Swapping of the contents can change the low and high frequencies, with low frequencies representing the general orientation and shape and high frequencies representing the sudden changes in the image like edges and fine details regarding the image. The next step involves performing the second level of decomposition with the new approximate coefficient matrix A_1 to obtain the second level of approximation coefficient matrix A_2 and detail coefficient matrices H_2, V_2 and D_2 . Similar set of operations are then performed on the coefficients obtained with second level of decomposition with the first step involving the diminishing of the A_2 values by dividing with M x N where M and N are the matrix dimensions of A_2. Next step involves the reversal of the coefficients V_2, H_2 and D_2 followed by the swapping of A_2 with V_2 and H_2 with D_2. In the last stage, two sets of Inverse discrete wavelet transform (IDWT) is performed, first using A_2, H_2, V_2 and D_2 to get the image Y_2, followed by performing the IDWT of Y_2, H_2, V_2 and D_2. Thus, in the proposed encryption method, only two levels of decomposition using DWT is performed on the target image, which itself makes the resulting encrypted image highly resistant to statistical attacks and also reduces the complexity of the system.

The detailed steps of encryption are discussed as below :

Step 1: Obtained an original image P to be encrypted, of size M * N. The approximation coefficient A_1 and detailed coefficients H_1, V_1 and D_1 of the original image P are computed with Discrete Wavelet Transform (DWT) using the Haar transform forming the first set of wavelet decomposition coefficients. Here, we have taken three standard images, 'barbra', 'Lena' and 'Lake' of size 256 * 256, as the original images to be encrypted.

Step 2: The approximation coefficient A_1 is diminished by dividing A_1 with the size of A_1, where as the detailed coefficients are reversed.

$A_1 = A_1 / (128 * 128)$
$H_1 = H_1 * (-1)$
$V_1 = V_1 * (-1)$
$D_1 = D_1 * (-1)$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5779
***Article Received**: 24 August 2022 **Revised**: 04 October 2022 **Accepted**: 19 October 2022*

Step 3: The contents of A_1 are swapped with V_1 and D_1 are swapped with H_1.

Step 4: The DWT of the diminished approximation coefficient A_1 is performed to obtain the approximation coefficient A_{2e} and detailed coefficients H_{2e}, V_{2e} and D_{2e} at the second level of wavelet decomposition.

Step 5: The same set of operations performed at the first level of decomposition is repeated in the second level. The approximation coefficient A_{2e} is diminished by dividing A_{2e} with its size

$A_{2e} = A_{2e} / (64 * 64)$
$H_{2e} = H_{2e} * (-1)$
$V_{2e} = V_{2e} * (-1)$
$D_{2e} = D_{2e} * (-1)$

Step 6 : The contents of A_{2e} are swapped with V_{2e} and D_{2e} are swapped with H_{2e}.The decomposition is repeated in the second level. The approximation coefficient A_{2e} is diminished by dividing A_{2e} with its size

$A_{2e} = A_{2e} / (64 * 64)$
$H_{2e} = H_{2e} * (-1)$
$V_{2e} = V_{2e} * (-1)$
$D_{2e} = D_{2e} * (-1)$

Step 6 : The contents of A_{2e} are swapped with V_{2e} and D_{2e} are swapped with H_{2e}.

Step 7: The swapping operation is followed by two levels of Inverse Discrete Wavelet Transform (IDWT). First step is to perform IDWT using the coefficients A_{2e}, H_{2e}, V_{2e} and D_{2e} to get the image Y_2.

Step 8: This is final step of encryption, to get the encrypted image 'E' by performing the IDWT using Y_2 from the previous step and the coefficients V_1, H_1 and D_1 obtained at step 3.

B. Proposed Decryption System

In the proposed decryption system, the first step involves performing the Discrete Wavelet Transform of the encrypted image to obtain the approximation coefficient matrix A_{d1} and the detailed coefficient matrices H_{d1}, V_{d1} and D_{d1} followed by the DWT of A_{d1} to obtain the second level of decomposition coefficients A_{d2}, H_{d2}, V_{d2} and D_{d2}. Next step involves the swapping of the contents of A_{d1} with V_{d1} and D_{d1} with H_{d1}. The third step involves reversing the detail coefficients V_{d1}, H_{d1} and D_{d1} and diminishing the approximation coefficient A_{d1} by dividing with the size of A_{d1}. This step is then followed by a similar sequence of operations ie; swapping of contents of A_{d2} with V_{d2} and H_{d2} with D_{d2}, followed by reversing the contents of H_{d2}, V_{d2} and D_{d2} and diminishing of A_{d2} by dividing with size of A_{d2}. The final step of decryption involves performing the IDWT using A_{d2}, H_{d2}, V_{d2} and D_{d2}, reversing the contents of V_{d2} and performing IDWT using A_{d1}, H_{d1}, V_{d1} and D_{d1}. Thus, reverse operation is performed on the encrypted image 'E' to get back the decrypted original image 'P'.

The detailed steps of decryption are discussed as below :
Step 1: The decryption operation starts with two levels of DWT operations, first computing the DWT of the encrypted image 'E' to obtain the approximation coefficient A_{d1} and detailed coefficients H_{d1}, V_{d1} and D_{d1} followed by the second level of DWT operation of A_{d1} to get the coefficients A_{d2}, H_{d2}, V_{d2} and D_{d2}.

Step 2: The two levels of DWT operations are followed by the swapping of the contents of A_{d1} with V_{d1} and D_{d1} with H_{d1}.

Step 3: Next step involves the reversal of H_{d1} and D_{d1} followed by retrieving the diminished approximation coefficient during encryption, by multiplying A_{d1} with size of A_{d1}.

$A_{d1} = A_{d1} * (128 * 128)$
$H_{d1} = H_{d1} * (-1)$

Fig. 1. From left to right, the figure represents the original standard image "Barbra", its encrypted and decrypted results using proposed system

$V_{d1} = V_{d1} * (-1)$
$D_{d1} = D_{d1} * (-1)$

Step 4: Next step is to swap the contents of A_{d2} with V_{d2} and D_{d2} with H_{d2}.

Step 5: Swapping operation is followed by the reversal of H_{d2}, V_{d2}, D_{d2} and retrieving of diminished approximation coefficient A_{d2} by multiplying it with size of A_{d2}.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5779
***Article Received**: 24 August 2022 **Revised**: 04 October 2022 **Accepted**: 19 October 2022*

$H_{d2} = H_{d2} * (-1)$
$D_{d2} = D_{d2} * (-1)$
$V_{d2} = V_{d2} * (-1)$
$A_{d2} = A_{d2} * (64 * 64)$

Step 6: The last step of decryption involves the two levels of IDWT and a reversal step. First is the computation of IDWT of coefficients A_{d2}, H_{d2}, V_{d2} and D_{d2} to get a 128 * 128 image Y_{d2} followed by assigning Y_{d2} to V_{d1} and finally the computation of the decrypted image D by computing the IDWT of coefficients A_{d1}, H_{d1}, V_{d1} and D_{d1}.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Several measures are used to access the quality of the encrypted and decrypted image obtained by the proposed encryption and decryption algorithm. Several mathematical and computational analysis needs to be performed to access the image quality. These analysis includes calculation of Mean Square Error or MSE and PSNR which represents Peak Signal to Noise Ratio [9]. Fig.1. shows the original standard image 'Barbra', its encrypted and decrypted versions using the proposed algorithm.

$$PSNR = 10\ log_{10}\ (\ L^2/MSE\ ) \quad (3)$$

Peak Signal to Noise Ratio (PSNR) is given by equation (3) with MSE defined as

$$MSE = (\ 1/N) * \sum_{i,j=0}^{N}\ (x_{ij} - y_{ij})(x_{ij} - y_{ij}) \quad (4)$$

where N represents the total number of pixels in the image and the i^{th} and j^{th} pixels in the original and decrypted image represented by x_{ij} and y_{ij} . L represents the dynamic range of the pixels which is equal to 255 for gray scale images. Both MSE and PSNR measures the quality of the decrypted images. Table 1 summarizes the PSNR values between the original and

Table.1. PSNR results of proposed work compared to other benchmark algorithms

Standard Image	Proposed work	S.Tedmore etal.	Sethi & Sharma
	PSNR (O-E)	PSNR (O-E)	PSNR (O-E)
Lena	0.0011	0.0017	0.036
Barbra	0.0053	0.0077	0.109
Lake	0.0021	0.0043	0.072

encrypted images using the proposed method and other benchmark algorithms and the results clearly indicates that the proposed method is better than other benchmark algorithms due to the low measurement values of PSNR between the original and encrypted images.

A. Statistical Analysis

A good cryptographic system needs to be statistically resistant to statistical attacks. The resistance of the system to such attacks can be found by performing the following analysis on the proposed system and also the encrypted and decrypted images obtained using the proposed cryptographic system.

1) Key

A symmetric key is used for encryption in the proposed work. When the algorithm uses same key for both encryption and decryption in cryptosystems, it forms the symmetric-key algorithm. In the proposed system, the available image details are used to design the key and so the symmetric key used is image dependent. In the steps 2 and 5 of the encryption process, the size of A_1 and A_{2e} are used as the encryption keys, whereas in the decryption process, the size of A_{d1} and A_{d2} are decryption keys which are same as that of the encryption keys. Since the size of images at intermediate stages are used as keys for the proposed method, there is no need for the storage of the key or its transmission are better and faster when compared to public key encryption system.

2) Correlation between adjacent pixels

In this test, the correlation between two adjacent pixels of both original and encrypted image is found out. First step is to randomly select from both the encrypted and original image around 10,000 pairs of adjacent pixels aligned horizontally, vertically and diagonally. Next step is to calculate the correlation coefficients of the selected pairs of adjacent pixels using equation (5)[10][11].

$$C_{xy} = \frac{COV(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}} * 100\ \% \quad (5)$$

$$\text{where, } \mathrm{COV(x,y)} = \frac{1}{\mathrm{P}}\ \sum_{1}^{\mathrm{T}}\big(\mathrm{x_i} - \mathrm{E(x)}\big)\big(\mathrm{y_i} - \mathrm{E(y)}\big) \quad (6)$$

$$\mathrm{E(x)} = \frac{1}{\mathrm{P}}\ \sum_{\mathrm{i=1}}^{\mathrm{P}} \mathrm{x_i} \quad (7)$$

$$\mathrm{E(y)} = \frac{1}{\mathrm{P}}\ \sum_{\mathrm{i=1}}^{\mathrm{P}} \mathrm{y_i} \quad (8)$$

$$\mathrm{V(x)} = \frac{1}{P}\sum_{i=1}^{P}(x_i - E(x_i))^2$$

Table.2. Correlation Coefficients of adjacent pixels in Original and Encrypted Images

Encryption Algorithm	Test Image	Horizontal		Vertical		Diagonal	
		Original	Encrypted	Original	Encrypted	Original	Encrypted
Proposed Method	Lena	0.928	0.0013	0.934	0.0031	0.973	0.0014
	Lake	0.998	0.0019	0.929	0.0011	0.934	0.0045
S. Tedmore etal.	Lena	0.919	0.0023	0.927	0.0042	0.962	0.0053
	Lake	0.987	0.0025	0.936	0.0015	0.927	0.0105
Sethi & Sharma	Lena	0.913	0.0031	0.920	0.0049	0.925	0.0062
	Lake	0.942	-0.0016	0.922	0.0036	0.887	0.0144

$$\mathrm{V(y)} = \frac{1}{P}\ \sum_{i=1}^{P}(y_i - E(y_i))^2 \quad (9)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5779
***Article Received**: 24 August 2022 **Revised**: 04 October 2022 **Accepted**: 19 October 2022*

x and y represent the gray-scale values of image pixels, and P represent the total number of pairs of pixels selected from image. The correlation between plain and encrypted image adjacent pixels are summarised in table 2. The proposed algorithm results in small values of correlation coefficients for the encrypted images when compared to other benchmark algorithms.

3) Histogram Analysis

The histogram of the original and the encrypted image is shown in fig.2.The figure clearly shows that the encrypted image histogram is totally different from that of the original image. The histogram of the original image is non-uniformly distributed whereas that of the encrypted image is left-shifted. Thus, the possibility of a statistical attack on the encrypted image is minimized due to insufficient data from the histogram of the encrypted image [12].

4) NPCR and UACI Analysis

In this, the resistance of the cryptosystem to a change in the just a single pixel of the plain image is calculated. The cryptosystem is said to resist differential attacks efficiently if a change in single pixel of the plain image can cause significant change in the pixels of the cipher image. The two common techniques used to find the influence of single-pixel change of the plain image on the cipher image are : (1) NPCR, Number of Pixels Change (2) UACI, Unified Average Changing Intensity [13][14]. NPCR refers to the rate of change of the number of pixels in the cipher image when a single pixel is changed in the plain image whereas, UACI refers to the average difference of intensities between the plain and the cipher image. NPCR and UACI.

$$\mathrm{NPCR} = \frac{\sum_{i,j=1}^{m,n} D(i,j)}{w \times h} * 100\ \% \qquad (10)$$

$$\mathrm{UACI} = \frac{1}{w \times h}\left[\sum_{i,j}^{m,n} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\ \% \qquad (11)$$

$$D(i,j) = \begin{cases} 1, & \text{if } C_1(i,j) = C_2(i,j) \\ 0, & \text{Otherwise} \end{cases} \qquad (12)$$

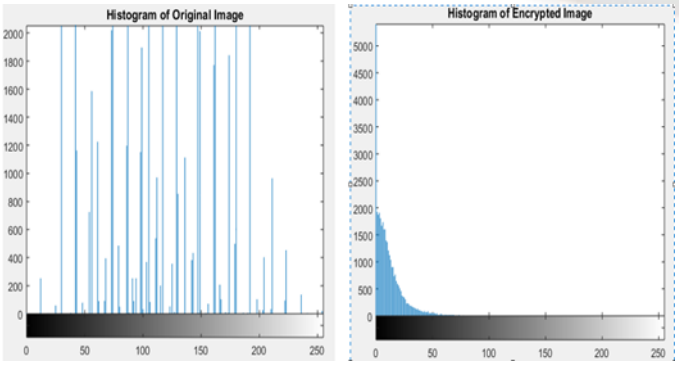

Fig. 2. From left to right, the figure represents the histogram of the original image "Barbra" and its encrypted form

Table 3 summarizes the NPCR and UACI results of standard images calculated using the proposed method and other benchmark algorithms. From the table 3, it is clear that the average values of NPCR and UACI mean values obtained using the proposed method are 99.99 % and 40 % respectively, which is better than other benchmark algorithms. The higher values of NPCR clearly indicates that by using the proposed method to encrypt, position of pixels are better randomized and that the system is highly resistant to differential attacks. Also, the quality of original image is preserved in the decrypted image since both the original and the decrypted image are identical, as indicated in figure 1.

5) Entropy

An image entropy represents the distribution of gray scale values in the image [15]. Entropy of a source or an image is determined using the equation (11)

$$H(S) = -\sum_{i=0}^{N-1} p(S_k) \log_2 p(S_k), \qquad (13)$$

where $p(S_k)$ is the possibility of presence of the symbol $p(S_k)$. Table 4 shows the original and corresponding encrypted image entropies for two standard images and also its comparison with the result obtained with other benchmark algorithms. The table indicates that the entropy values are closer to 8 bits indicating a negligible leakage in the information and resistance of the cryptosystem against entropy attacks.

V. Conclusion

A loss-less cryptosystem based on value transformation, visual transformation and pixel permutation is presented in the article. The original image is initially transformed into frequency domain using DWT and consequent low frequency and high frequency sub-bands are changed suitably into a form to obtain a secure encryption system. Reverse procedure is done in the decryption process to get back the original image with minimum distortion. The simulation results indicated a high efficiency of the system and proved that the proposed system is secure and highly resistant to statistical attacks. The simulation results are also compared with benchmark algorithms to prove the efficiency of the proposed work.

Table. 3. NPCR and UACI of Standard Images

Standard Images	Proposed Method		S. Tedmore etal.		Sethi & Sharma	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.981	38.99	99.941	38.981	95.124	20.113
Barbra	99.992	39.63	99.961	39.847	97.586	12.431
Lake	99.982	39.01	99.941	38.981	97.316	34.124

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5779
***Article Received**: 24 August 2022 **Revised**: 04 October 2022 **Accepted**: 19 October 2022*

Table. 4. Entropy Results of Standard Images

Algorithm	Entropy of the Encrypted Images	
	Lena	Boat
Proposed Work	7.999	7.995
S. Tedmore etal.	7.997	7.996
Sethi & Sharma	7.989	6.574

REFERENCES

[1]. Y. Chen, Comment on ‘‘Cheating prevention in visual cryptography’’, IEEE Trans. Image Process; vol.21 no.7, 3319–3323, 2012

[2]. X. Zhang, Scalable coding of encrypted images, IEEE Trans. Image Process;vol.21, no.6, 3108–3114, 2012.

[3]. G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Elsevier Opt. Commun. vol.284, no.12, 2775–2780, 2011.

[4]. A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Elsevier Commun. Nonlinear Sci. Numer. Simul., vol.17 , no.7, 2943–2959, 2012

[5]. M. Bani-Younes, A. Jantan, Image encryption using block-based transformation algorithm, Int. J. Comput. Sci. ,vol. 35, no. 1,pp. 15–23, 2008.

[6]. C. Samson and V. Sastry, “A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform”, Int.l J. of Advanced Comput. Sci. App, Vol. 3, no. 9, pp. 178-183, 2012.

[7]. C. Pang, An image encryption algorithm based on discrete wavelet transform and two dimension cat mapping, in: Int. Conf. on Networks Security, Wireless Communications and Trusted Computing, vol. 2, IEEE Xplore digital library, pp. 711–714, 2009

[8]. L. Krikor, S. Baba, T. Arif, Z. Shaaban, Image encryption using DCT and stream cipher, Eur. J. Sci. Res, vol. 32, no.1, 47–57, 2009.

[9]. S. Tedmori and N. Al-Najdawi, “Image Cryptographic Algorithm Based on the Haar Wavelet Transform”, Elsevier Information Sciences, vol. 269, pp. 21-34, 2014

[10]. Z. Liu, J. Dai, X. Sun, S. Liu, Triple image encryption scheme in fractional Fourier transform domains, Elsevier Opt. Commun., vol.282, no. 4, pp.518–522, 2009.

[11]. M. Khan and F. Masood, ‘‘A novel chaotic image encryption technique based on multiple discrete dynamical maps,’’ Multimedia Tools Appl., vol. 78, no. 18, pp. 26203–26222, 2019.

[12]. R. Ye, A novel chaos-based image encryption scheme with an efficient permutation–diffusion mechanism, Elsevier Opt. Commun., vol. 284, pp.5290– 5298, 2011.

[13]. N. Sethi, D. Sharma, Novel method of image encryption using logistic mapping, Int. J. Comput. Sci. Eng., vol.1, no.2, 115–119, 2012.

[14]. Kaur, M.; Kumar, V. A comprehensive review on image encryption techniques. Arch. Comput. Methods Eng., vol.27, pp.15–43, 2020.

[15]. Khan, J.S.; Ahmad, J. Chaos based efficient selective image encryption. Multidimens. Syst. Signal Process., vol.30, pp. 943–961, 2019.