j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

ANEW ARCHITECTURE OF KEY GENERATION USING DWT FOR IMAGE ENCRYPTION WITH THREE LEVELS ARNOLD TRANSFORM PERMUTATION

Qutaiba K. Abed [1], Waleed A. Mahmoud Al-Jawher[2]

[1]*Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq.*

[2] *College of Engineering, Uruk University, Baghdad, Iraq.*

phd202130682@iips.icci.edu.iq

Abstract The security of image transmission is an important issue in digital communication. As well as it is necessary to preserve and protect important information for several applications like military, medical and other services related to high confidentiality over the Internet or other unprotected networks. In this paper a proposed encryption scheme was introduced that using Lorenz system with a circular convolution and discreet cosine transform (DCT). The diffusion process was achieved using three levels of Arnold transform permutation: - namely, block level, inside each block and pixel level. The image was divided into blocks of sizes 8x8 pixels and shuffle by applying Fisher-Yates permutation image pixels. The DCT was applied to each block and multiplied by the H kernel matrix to achieve the circular convolution. Next the logistic map is used for diffusion to get the cipher image. A new key generation method is applied in order to produce the key values for generating the chaos numbers sequence. Finally applying the discreet wavelet transform (DWT) to the image will produced four quarters (LL, LH, HL and HH). The cosine of each pixel in the LL and HH quarters were computed. The sine of each pixel in the LH and HL quarters were also computed in order to generate the keys for the chaos sequence. By using this way of keys generation in every image, the differential attack possibility will be negligible.

Crossref 10.36371/port.2022.3.6

Keywords: *Convolution diffusion, Fisher Yate permutation, Sine and Cosine function, Arnold transform, permutation for Pixel level, DCT and DWT*

1. INTRODUCTION

Nowadays, image security is becoming increasingly important as more and more confidential images are transmitted over public Internet or stored in a third party. In this respect, various image cryptosystems have been suggested because encryption is recognized as an effective and direct technique to keep private information safe. With the rapid development of digital image processing technology, people pay more and more attention to improve the security of information [1]. Chaotic systems have many features suitable for cryptography, including pseudo randomness, initial value sensitivity, parameter sensitivity, periodicity, and unpredictability. Therefore, in recent years, the use of chaotic systems to study encryption algorithms has become one of the hot spots in the field of computer science and cryptography [2].

Chaotic system has many excellent intrinsic properties, such as ergodicity, aperiodicity, high sensitivity to initial conditions and control parameters and random-like behaviors. Therefore, researchers have proposed many image encryption algorithms based on chaotic systems [2–21]. The typical ciphers based on chaotic map can be partitioned into two stages, permutation and diffusion [3].

From several research works, it has been inferred that performing permutation only within a sub block alone cannot give acceptable security. Chaotic sequence provides better randomness to improve security. N time's permutation and M times' diffusion will decrease the potential in cryptanalysis. Both permutation and diffusion are important processes in increasing the security of the cipher. With these facts, the following steps have been taken for image security which are cited as contributions to this work, an actual image-related key generation technique is used to reduce the risk of differential attack [4]

In [5], an image encryption based on one-time keys is proposed. In [6], a novel chaotic block image encryption algorithm based on dynamic random growth technique is proposed. Although the schemes adopt some measures in the encryption process to improve security, but they cannot resist chosen plaintext attack and chosen-ciphertext attack totally. To avoid attackers crack cryptosystems by using the order from top to bottom and from left to right, Wang et al. proposed dynamical pixel order for diffusion and sub-images

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

division method [7]. Belazi et al. [8] proposed a new chaos-based partial image encryption scheme which encrypts only the requisite parts of the sensitive information in frequency domain of Lifting-Wavelet Transform (LWT) based on hybrid of chaotic maps and a new S-box. Liu et al. [9] proposed a fast image encryption algorithm. In this algorithm, the confusion and diffusion processes are combined for one stage. Wang et al. [10] proposed a novel hybrid color image encryption algorithm using two complex chaotic systems to enhance the security and enlarge key space of color image encryption. In [11–16], a variety of image encryption algorithms using bit-level permutation have been proposed due to the advantages of bit-level permutations, which can change the position and value of a pixel simultaneously. In [6], a new bit-level encryption algorithm based on the spatiotemporal non-adjacent coupled map lattices which makes it possible for any bit in pixels to break the limit of its bitplane without extra space in permutation process .

Take the DWT to the input image and apply computation to get the initial keys for Lorenz chaos and logistic map[31-40]. Three layered, pixel level of Arnold transform and Fisher-Yates scrambling method is employed to randomize the pixel values. A circular convolution is performed to improve security, multiplication operation is applied in frequency domain to get the result of the circular convolution, and logistic map is used to apply diffusion to get the final cipher image.

2. CHAOTIC MAPS

Chaotic maps are non-linear dynamical systems that behave chaotically in a manner under certain parameters and initial values. The randomness in the chaos sequence is needed for image encryption to randomize the image by permutation/diffusion. It mainly secures the image from the possibility of pattern attacks [18, 4]. Chen chaotic system can be described by

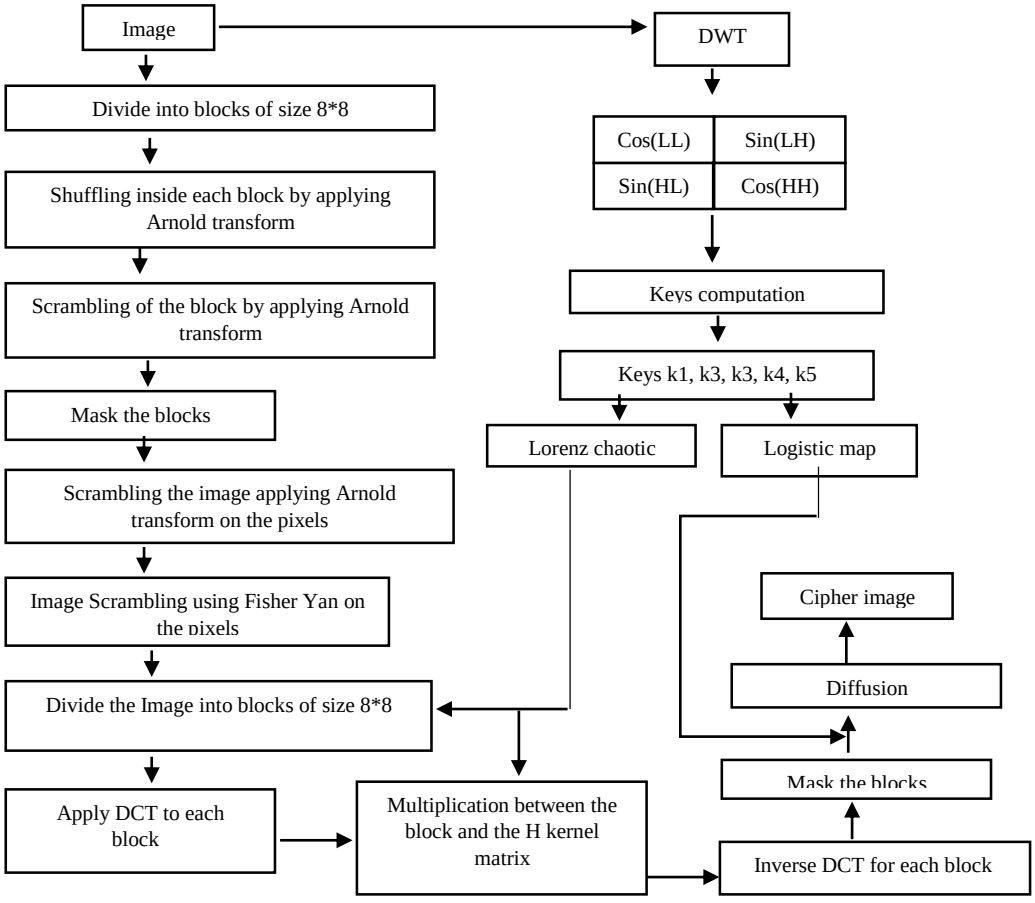
$$\frac{dx}{dt} = \sigma(y - x) \quad , \quad \frac{dy}{dt} = x(\rho - z) - y$$

$$\frac{dz}{dt} = x * y - \beta * z \qquad (1)$$

Where σ, ρ and β are control parameters, when σ =35, ρ =3, β=28, the system represents chaotic characteristics.The Logistic chaotic map is a degree 2 polynomial and exhibits chaotic behavior under certain parametric values. The equation for the map sequence generator is expressed in Equation (2)

$$K_{n+1} = r*K_n*(1 - K_n) \qquad (2)$$

Where K_n is the value between 0 and 1. r is the parameter within the interval [0,4].



Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

3. THE PROPOSED ENCRYPTION SYSTEM

In this encryption method the Discreet Wavelet Transform (DWT) is first calculated for the input natural image, where as a result of applying the Discreet Wavelet Transform (DWT), we will obtain four divisions of the image, which are LL, LH, HL and HH, and then operations are applied to these four parts. Sine for LL, HH and Cos for LH, HL are calculated, in order to compute the calculation to obtain the five keys K1, K2, K3, K4, K5 that can use as keys for Lorenz chaotic and logistic map. Then the same as the original natural image have been divided into 8×8 blocks. Three levels of Arnold transform permutation have been performed in order to ensure security. In the first level, Arnold transform permutation is applied inside each block. In the second level, Arnold transform permutation is performed on the all blocks in order to scramble the 8×8 blocks into another places. Then, the blocks have been masked into a single image and on the whole Arnold transform permutation is applied in the third level. Each Level is permuted by Arnold transform manner for n times. Fisher-Yates is performed for all pixels to scramble all image. Divide the image to blocks each 8*8 pixels and the apply DCT to each block after that convolute the each block with the H kernel matrix then apply IDCT to get the result. Applying diffusion to get the final cipher image. This can be describe the following procedure.

1- Input a natural image size (256*256)

2- Obtain the DWT which result into four quarters namely; LL, LH, HL and HH.

3- calculate the sine of each pixel in LH and HL quarters

4- calculate the cosine of each pixel in LL and HH quarters

5- select 64 octal values from the result of step 4 above using the following set of equations

$$n1=f1+f5+f9+\ldots\ldots\ldots+f61$$

$$n2=f2+f6+f10+\ldots\ldots\ldots+f62$$

$$n3=f3+f7+f11+\ldots\ldots\ldots+f63$$

$$n4=f4+f8+f12+\ldots\ldots\ldots+f64$$

$$n5=f1+f3+f5+\ldots\ldots\ldots+f63$$

$$n6=f2+f4+f6+\ldots\ldots\ldots+f64$$

Where fi represent the value of the pixel from the processed image

6- Calculate the following parameters

$$W=((n1+n2)/256)+(n5/n3)$$

$$X=((n3+n4)/256)+(n6/n2)$$

$$Y=((n1+n3)/256)+(n5/n4)$$

$$Z=((n2+n3)/256)+(n6/n1)$$

7- Calculate the five initial keys necessary as initial keys necessary for Lorenz chaos and logistic map generation

$$K1=\text{mod}(W+X, 256)/256$$

$$K2=\text{mod}(Y+Z, 256)/256$$

$$K3=\text{mod}(W+X+Y, 256)/256$$

$$K4=\text{mod}(X+Y+Z, 256)/256$$

$$K5=\text{mod}(X+Y, 3)$$

Where the K1,K2,K3,K4 and K5 represent the keys for the Lorenz chaos

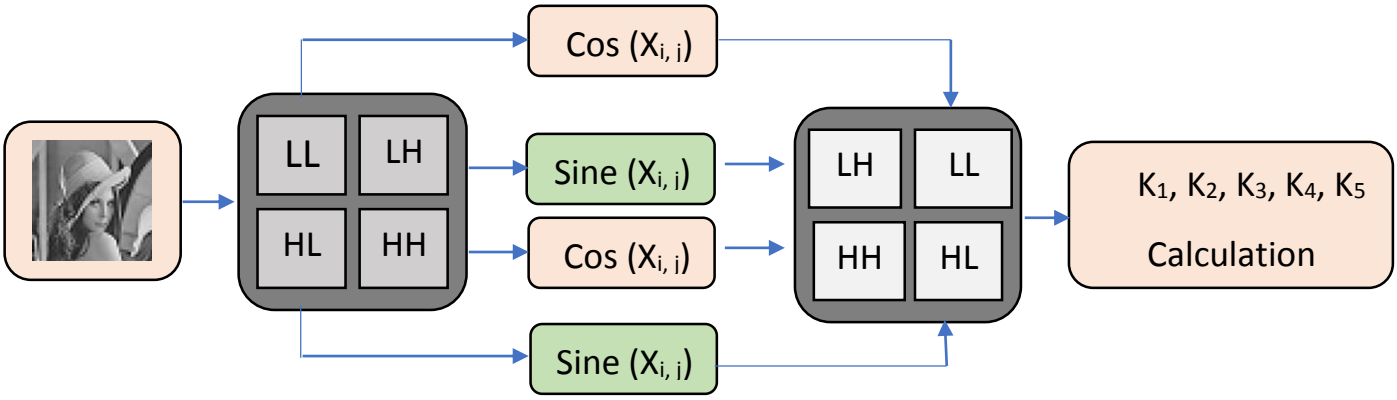


Figure 2: *depict the process of the keys generation*

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

8- Divide the image into 8*8 blocks

9- Applying three levels of permutation using Arnold transform as following:-

a- applying Arnold transform on the wavelet coefficient within each block

b- Applying Arnold transform on the index of the blocks.

c- Applying Arnold transform on an image wavelet coefficient of 256*256 dimension.

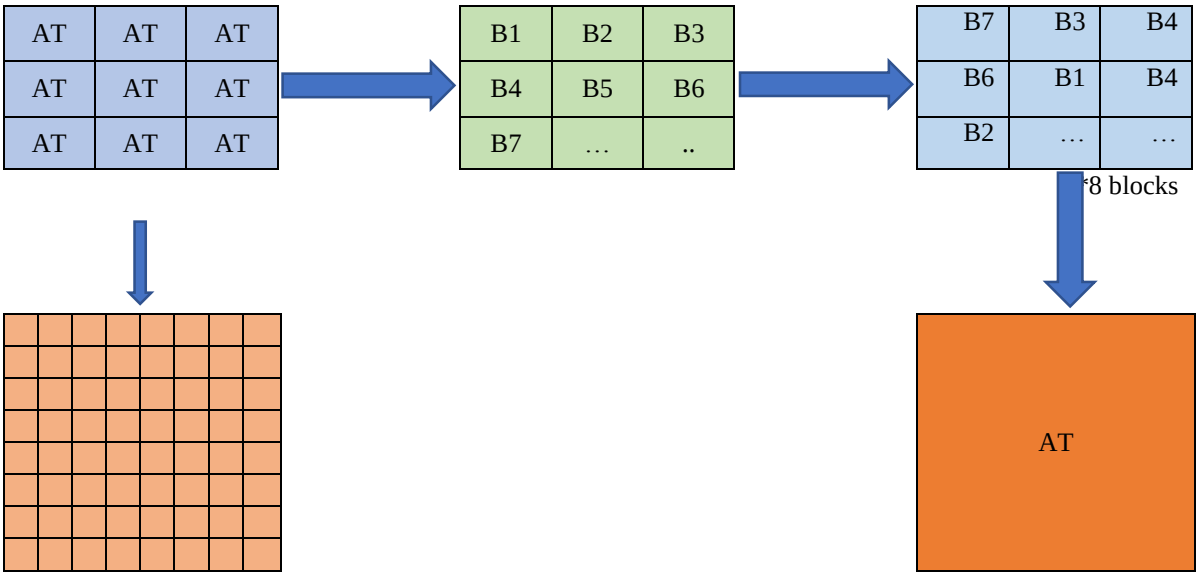


Figure 3: *Show the thee level Arnold Transform scrambling*

10- applying fisher Yates permutation for pixel shuffling randomly using the following procedure:

a- In each position starting from the end of the vector

b- The position index is taken in every loop

c- The map sequence value is taken as a random value and change with end position to get the new sequence.

d- Shift to the next position and new value is taken as another position.

e-Repeat the process to all position to get the scrambled image

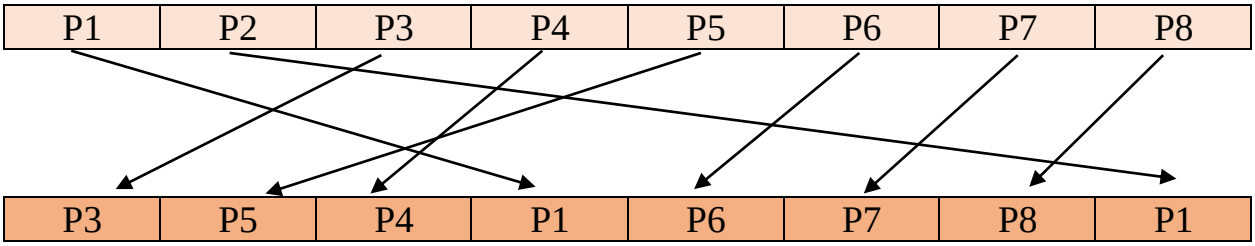


Figure 4*: Depicts the Fisher Yates permutation*

.

11- Apply the convolution on the H kernel matrix using the following steps:

a- H kernel matrix size (8*8) generated by Lorenz chaotic

b- Divide the input image into many blocks each size 8*8 bytes

c- Apply DCT to each block

d- Multiply each block with the H kernel matrix size 8*8 to get the new block

e- apply IDCT for the blocks

f- Repeat this process for all blocks in order to get the cipher image

12- Quantify the result to make it between [0-255].

13- Diffuse the result with the logistic map number Cipgher=im xor logistic_map (i, j)

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

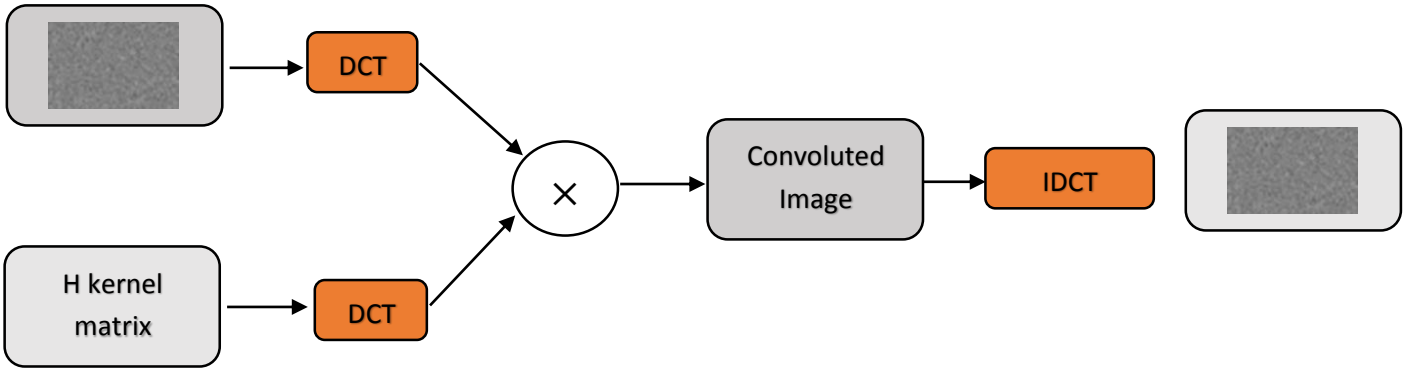


Figure 5: *Convolution with the H kernal matrix*

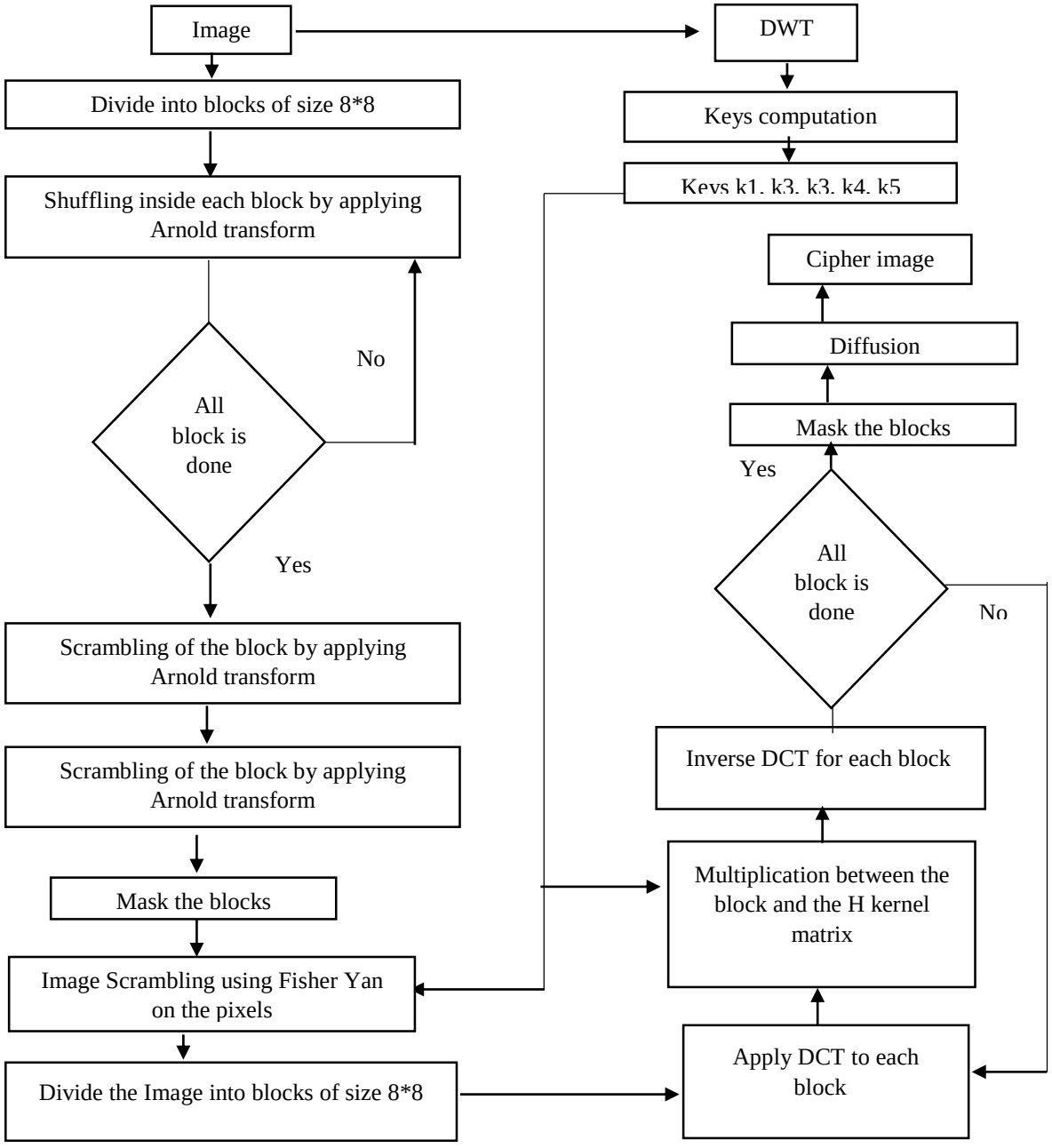


Figure 6: *The overall flowchart of the proposed encryption system.*

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

The Decryption Method

The decryption way of the system can be performed by reversing the order of the encryption process. Inverse the diffusion, then Inverse circular convolution is applied. After that, inverse Fisher-Yates permutation is applied. Then Inverse Arnold transform permutation is performed to get the decrypted image. Figure 7 shows permuted image, diffused image and decrypted image.

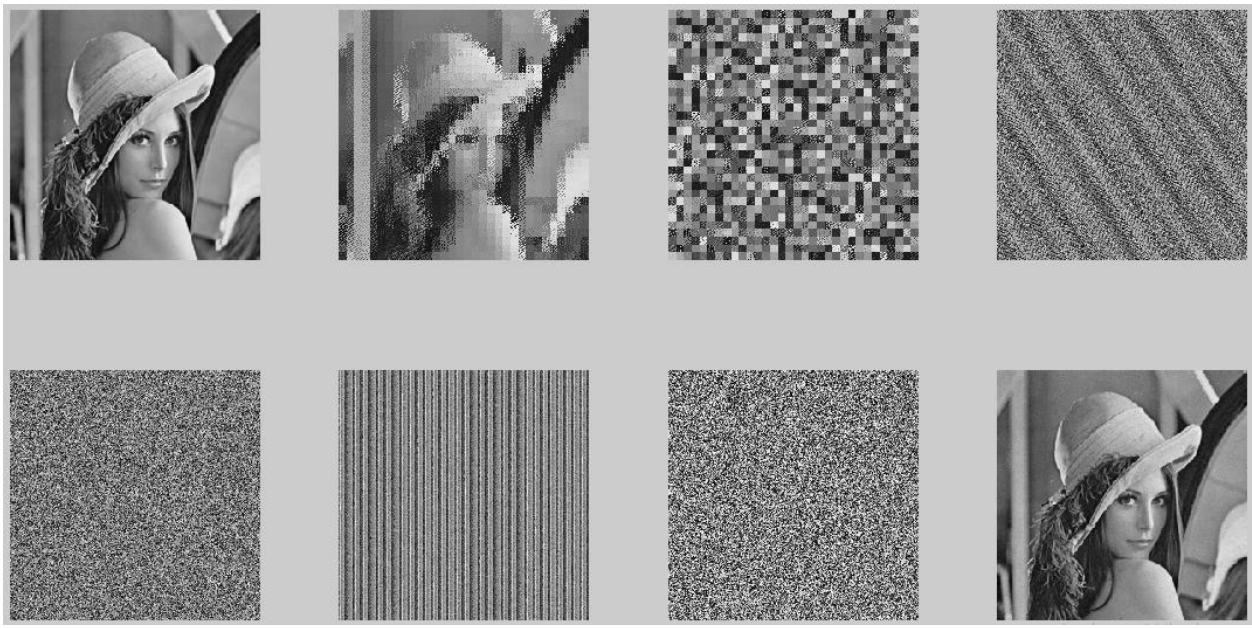


Figure 7*: shows permuted image, diffused image and decrypted image.*

4. The Results of the proposed system

This part discusses the results obtained from the simulation of the proposed encryption system. As shown in Figure 7, the effects of encryption and decryption are visually displayed. Five 256×256 grayscales Lena, Baboon, peppers, Barbara and Gold-hill are used as original images. It is all the plain images are encrypted into cipher images. The cipher images are noise like images without carrying any visual information. Besides, the decrypted images look much the same visually as their original counterparts.

4.1 The Analysis of the Key Length

The security level of the cryptosystem mainly depends on the key. The key length of the system must be as large as to prevent an exhaustive attack. In the proposed algorithm, five initial keys are needed to generate chaotic sequences.10^{-15} is the precision of these numbers then a total of 10^{90} which is greater than 2^{100}. Hence brute force attack cannot be attempted.

4.2 Analyzing the Correlation Coefficient

The relationship between the nearby pixel values is one of the ways to get the information from the encrypted image. In normal images, the correlation coefficient value is close to 1, whereas in encrypted images, the correlation coefficient value is close to 0. If it is nearer 0, then the possibility of getting any information through the correlation among pixels is very low. The Correlation Coefficient *(CC)* is measured using Equation (3)

$$CC = \frac{D1((x-D1(x))(y-D1(y)))}{\sqrt{U1(x)U1(y)}} \quad (3)$$

Where D1 (x) and U1(y) are the gray level expectation and variance, respectively. Figure (3) illustrates the close statistical relationship between the pixels in the original image in all directions, where all pixels are concentrated in one area. The pixels are dispersed throughout the region. Table 1 shows the *CC* values of cipher images. Table 2 compares the *CC* value of the proposed solution with existing solutions. H1, V1 and D1 in Tables 1 and 2 denote the horizontal, vertical and diagonal correlation values, respectively. Obtained results of *CC* outperform the existing solutions.

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

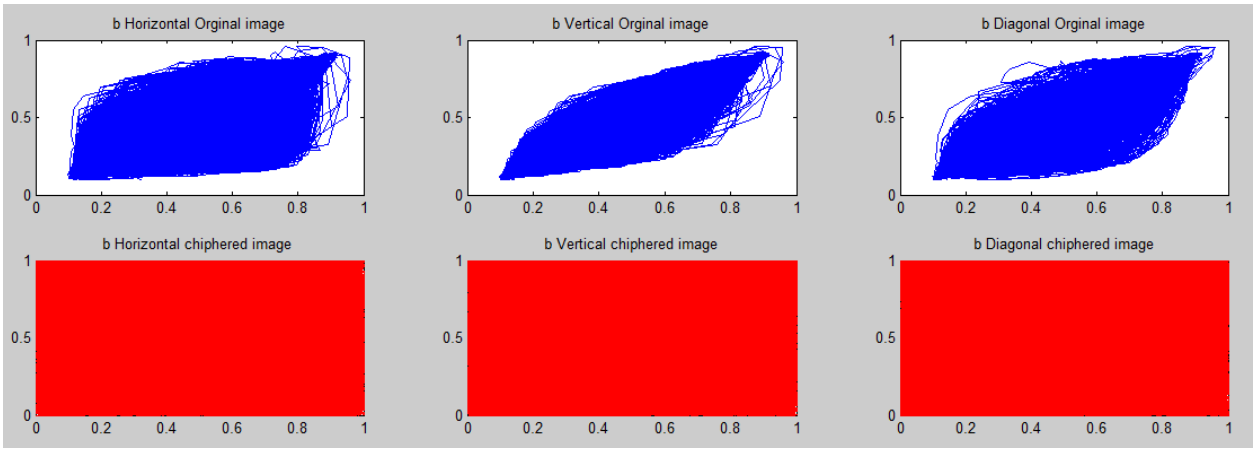


Figure 8: *Correlation distribution of plain and cipher image*

Table 1 *shows the CC values of cipher images*

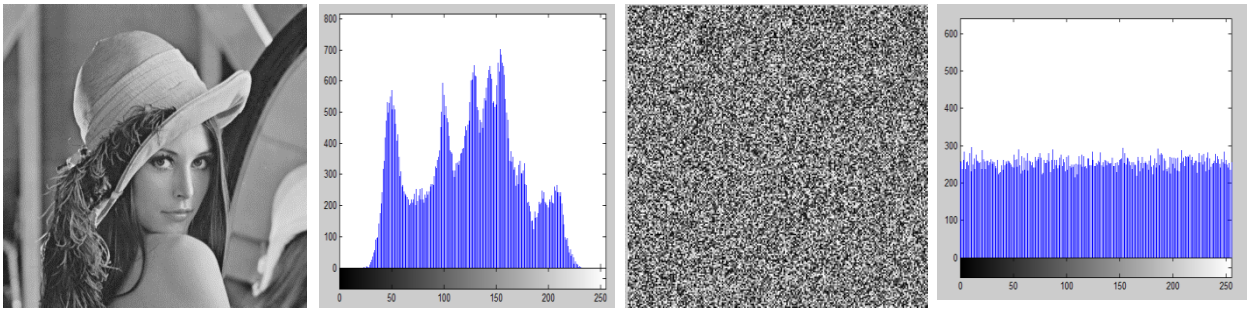
Direction	Vertical		Horizontal		Diagonal	
Image Type	Plain	Cipher	Plain	Cipher	Plain	Cipher
Lena	0.9850	0.0071	0.9719	-0.0001	0.9593	0.0056
Baboon	0.7586	0.0034	0.8665	0.0005	0.7261	-0.0016
peppers	0.9783	-0.0006	0.9810	0.0051	0.9631	-0.0000
Barbara	0.9619	-0.0001	0.9415	0.0005	0.9214	0.0032
Gold-hill	0.9743	-0.0006	0.9710	-0.0003	0.9511	0.0068

Table 2: *compares the CC value of the proposed solution with existing solutions*

Direction	**Vertical**	**Horizontal**	**Diagonal**
Ref[19]	-0.0296	-0.0050	-0.0230
Ref[20]	-0.0299	-0.0121	-0.0477
Ref[21]	0.0016	-0.0088	-0.0254
proposed	0.0071	-0.0001	0.0056

4.3 The Pixels Distribution

Histogram analysis is one of the most crucial statistical tests for evaluating the resistance of encryption algorithms to statistical analysis attacks. Graphically describing the distribution of pixel density, the histogram provides a comprehensive description of the image's content. Consequently, the normal image histogram and the encrypted image histogram must be fundamentally distinct, with the normal image histogram containing multiple peaks and vertices and the encrypted image histogram being flat, which helps to conceal the pixel density distribution information from attackers [22-25]. Figure 9 depicts the histogram of the normal and encrypted images generated by the proposed method, which demonstrated an effective outcome.

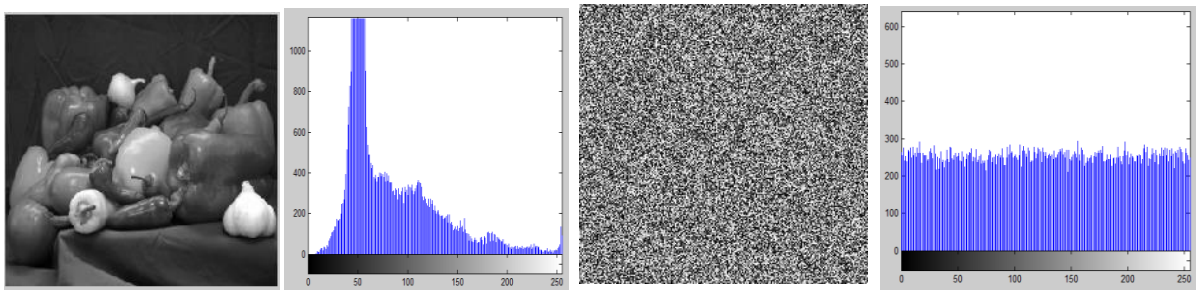


Plain and Encrypted Lena image

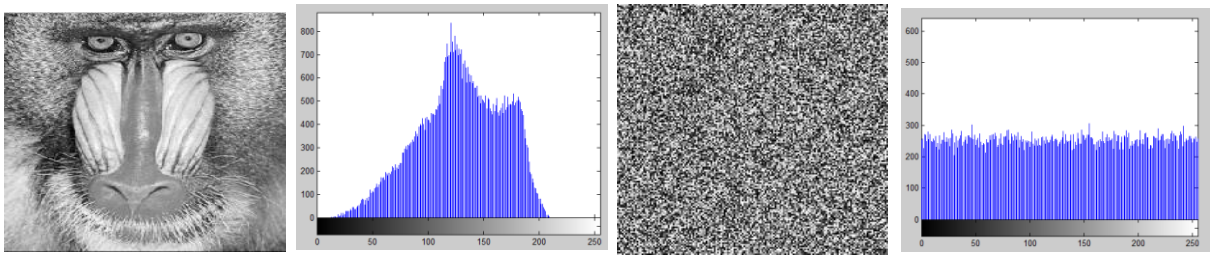
Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

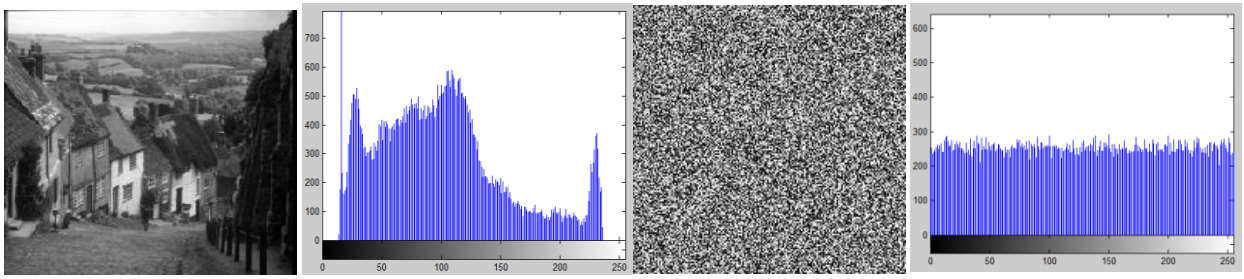
Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022



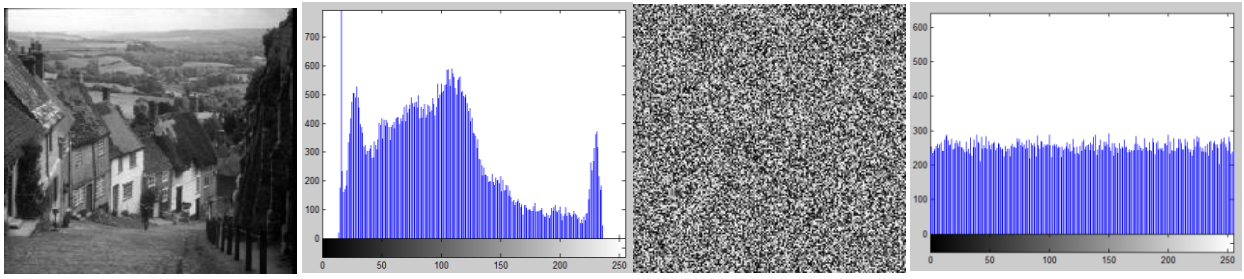
Plain and Encrypted Peppers image



Plain and Encrypted Baboon image



Plain and Encrypted Baboon image



Plain and Encrypted Gold-hill image

Figure 9: *depicts the histogram of the normal and encrypted images*

4.4 Local Entropy

Local entropy values are calculated to analyze the strength of the diffusion with the blocks of the encrypted image. Information entropy can be used as an indication of randomness for the plain and scrambling images. Its value should be larger for scrambled images. Ideally, it should be equal to 8 for every channel of an RGB color image [26]. A signal's information entropy can be calculated as in equation (4).

$$\text{entropy} = -\sum_{m=0}^{2N-1} q(m)\log_2 q(m) \quad (4)$$

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

Table 3: Entropy information examination results for five test images using the proposed system.

Image Type	Measure
Lena	7.9974
Baboon	7.9971
peppers.png	7.9976
Barbara	7.9974
Gold-hill	7.9975

Table 4: *Comparing the evaluation results of the proposed chaotic map to those of other method*

image	Lena	Peppers
Ref[27]	7.9973	7.9975
Ref[28]	7.9972	7.9974
Ref[29]	7.9976	7.9973
Ref[30]	7.9993593	7.9994499
Proposed	7.9974	7.9976

4.5 Quality Metrics Analysis (PSNR, MSE and MSSIM)

The degree of irregularity is measured using PSNR and MSE values. PSNR value should be as low as possible to get the encryption to be effective. Similarly, the MSE value should be as high as possible. The PSNR and MSE are calculated using Equations (5) and (6),

$$PSNR = 10 * log_{10} * \frac{255*255}{MSE} \quad (5)$$

$$MSE = \frac{1}{L*K}\sum_{i=1}^{k} \sum_{j=1}^{L}(p(i,j) - c(i,j)^2 \quad (6)$$

Where K, L is the size of original image, p (i, j) is the original image, and c(i, j) is the encrypted image. The higher value of MSE represents better encryption quality. This MSE analysis is a useful test for a plain image and encrypted image with pixel values in the range of [0–255]. The PSNR (expressed in logarithmic scale and decibels) determines the ratio between the maximum possible power of a signal and the power of distorting noise that affects the quality of its representation.

The Mean Structural Similarity Index (MSSIM) indicates the degree of similarity between two images, and it is closer to 1 means the more similar the images are. MSSIM can be calculated by

$$SSIM(P,D) = \frac{2*\mu p*\mu d+c1}{\mu^2 p+\mu^2 d+c1} * \frac{2*\sigma p*\sigma d+c2}{\sigma^2 p+\sigma^2 d+c2} * \frac{\sigma pd+c3}{\sigma p\sigma d+c3} \quad (7)$$

$$\mathrm{MSSIM}(\mathrm{P},\mathrm{D}) = \frac{1}{w}\sum_{i=1}^{w} SSIM(Pi, Di) \quad (8)$$

where W = 64, P and D are sequences of the original and decrypted images, μp and μd are the mean values of P and D, σp and σd are the variances of P and D, σpd is the covariance between P and D. Additionally, c1, c2, c3 are three constants $c1 = (k1*t)^2$, $c2 = (k2*t)^2$, c3 = c2/2, t= 255, k1 = 0.01 and k2 = 0.03.

Table 5 *shows the PSNR, MSE and SSIM values.*

Image Type	PSNR	MSE	SSIM
Lena	45.9317	7772.05	0.9915
Baboon	25.4270	6867.86	0.9707
peppers	40.2647	9723.7	0.9930
Barbara	31.3811	10264.66	0.9917
Gold-hill	33.0163	9280.47	0.9935

4.6 Noise attack analysis

Images are susceptible to various kinds of noise pollution during transmission. “Lena” and “Pepper” were used to test the resistance of this scheme to Salt and Pepper Noise (SPN) and Speckle Noise (SN) attacks. The decrypted images after adding SPN with the intensity of 0.00001, 0.00003, 0.0005 and 0.0007, respectively, Table 10 shows the corresponding PSNR values for these decrypted images. Both images had a fine PSNR values when exposed to SPN from 0.00001 to 0.00007. It means that our scheme has strong defense ability against SPN. On the other hand, the visual effect of decrypted

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

images is distinctly impacted when attacked under SN. But under SN attacks of limited intensity, the main information can be recognized from decrypted images. Therefore, it can be concluded from the experimental results that this algorithm can resist noise attacks.

Table 6 shows the PSNR values

	intensity	0.00001	0.00003	0.00005	0.00007
Salt and pepper	Lena	45.9317	45.9317	26.9207	28.6046
	Baboon	24.0800	40.7771	28.8744	30.5872
	intensity	0.00001	0.00003	0.00005	0.00007
Speckle	Lena	27.3732	28.5419	28.2337	27.0075
	Baboon	28.8050	28.9004	28.1387	28.6562

5. CONCLUSION

An encryption scheme to protect the image files has been proposed. The versatility of the proposed scheme, the Algorithm has been tested with standard analyses and tests such as Correlation coefficient, Histogram analysis, PSNR and MSE. The results obtained from the analysis of the cipher image are satisfactory and outperform when compared with existing encryption schemes. Fisher-Yates used for permutation in order to add further security. In this proposed system, three-layer permutation is performed to enhance security. Circular convolution layer are used for additional security, which is employed in substitution. And the last process is diffusion with keys to get the last encrypted image. Moreover, the used security measurements and computer simulation confirmed that the system are able to provide better protection against statistical, differential, and brute force attacks, where the algorithm based on circular convolution, Lorenz and logistic map Secret Keys has strong encryption procedures and high computational speed, and can overcome common weaknesses found in encryption algorithms based on other chaotic systems

REFERENCES

[1] Ping, Ping, et al. "Designing permutation–substitution image encryption networks with Henon map." Neurocomputing 283 (2018): 53-63.

[2] Wang, Xingyuan, Wenhua Xue, and Jubai An. "Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of household." Chaos, Solitons & Fractals 141 (2020): 110309.

[3] Li, Yueping, Chunhua Wang, and Hua Chen. "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation." Optics and Lasers in Engineering 90 (2017): 238-246.

[4] Devipriya, M., M. Sreenivasan, and M. Brindha. "Reconfigurable Architecture for Image Encryption Using a Three-Layer Artificial Neural Network." IETE Journal of Research (2022): 1-14 .

[5] Liu HJ, Wang XY. Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 2010;59:3320–7.

[6] Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015;66:10–8.

[7] Wang XY, Zhang YQ, Liu LT. An enhanced sub-image encryption method. Opt Lasers Eng 2016;86:248–54.

[8] Belazi A, El-Latif A, Diaconu A, Rhouma R, Belghith S. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 2017;88:37–50.

[9] Liu WH, Sun KH, Zhu CX. A fast image encryption algorithm based on chaotic map Opt Lasers Eng 2016;84:26–36.

[10] Wang LY, Song HJ, Liu P. A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt Lasers Eng 2016;77:118–25.

[11] Zhu ZL, Zhang W, Kwok-wo W. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 2011;181:1171–86.

[12] Teng L, Wang XY. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt Commun 2012;285:4048–54.

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. (2022). Anew Architecture Of Key Generation Using Dwt For Image Encryption With Three Levels Arnold Transform Permutation. Journal Port Science Research, 5(3), 166–177. https://doi.org/10.36371/port.2022.3.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 5, No:3. 2022

[13] Fu C, Lin BB, Miao YS, Liu X, Chen JX. A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 2011;284:5415–23.

[14] Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284:3895–903.

[15] Wang XY, Zhang HL. A color image encryption with heterogeneous bit permutation and correlated chaos. Opt Commun 2015;342:51–60.

[16] Xu L, Li Z, Li J. A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 2016;78:17–25.

[17] Zhang YQ, Wang XY. A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 2015;26:10–20.

[18] Luo, Yuling, et al. "An image encryption scheme based on block compressed sensing and Chen system." (2022.(

[19] Abdullah, Hamsa A.; Abdullah, Hikmat N.; Mahmoud Al-Jawher, Waleed A. (2019). A hybrid chaotic map for communication security applications. International Journal of Communication Systems, (), e4236–. https://doi:10.1002/dac.4236

[20] Ali Akram Abdul-Kareem, Prof. Waleed Ameen Mahmoud Al-Jawher(2022) "WAM 3D Discrete Chaotic Map for Secure Communication Applications" Proceeding of 3rd International Conference on Optics, Photonics and Lasers, 20-21 September, 2022 .

[21] Belqassim Bouteghrine;Camel Tanougast;Said Sadoudi; (2021). Novel image encryption algorithm based on new 3-d chaos map. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-021-10773-8

[22] Hanif, Muhammad; Naqvi, Rizwan Ali; Abbas, Sagheer; Khan, Muhammad Adnan; Iqbal, Nadeem (2020). A Novel and Efficient 3D Multiple Images Encryption Scheme Based on Chaotic Systems and Swapping Operations. IEEE Access, (), 1–1. https://doi:10.1109/access.2020.3004536

[23] Ali Momeni Asl;Ali Broumandnia;Seyed Javad Mirabedini; (2021). Scale Invariant Digital Color Image Encryption Using a 3D Modular Chaotic Map. IEEE Access, () –. https://doi:10.1109/access.2021.3096224

[24] Bashir, Zia; Iqbal, Nadeem; Hanif, Muhammad (2020). A novel gray scale image encryption scheme based on pixels' swapping operations. Multimedia Tools and Applications, (), –. https://doi:10.1007/s11042-020-09695-8

[25] Xiaoliang Qian;Qi Yang;Qingbo Li;Qian Liu;Yuanyuan Wu;Wei Wang; (2021). A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques. IEEE Access, (), –. https://doi:10.1109/access.2021.3073514

[26] DEMİRTAS, Mehmet. "A Color Image Scrambling Method Based on Zigzag Transform and Cross-channel Permutation." Avrupa Bilim ve Teknoloji Dergisi 36: 91-95.

[27] Xu, Lu, et al. "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion." Optics and Lasers in Engineering 91 (2017): 41-52.

[28] Wang, Xingyuan, et al. "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level." Optics and Lasers in Engineering 125 (2020): 105851.

[29] Luo, Yuling, et al. "Image encryption scheme by combining the hyper-chaotic system with quantum coding." Optics and Lasers in Engineering 124 (2020): 105836.

[30] Malik, Dania Saleem, and Tariq Shah. "Color multiple image encryption scheme based on 3D-chaotic maps." Mathematics and Computers in Simulation 178 (2020): 646-666.

[31] Qutaiba K.Abed, Prof. Waleed Ameen Mahmoud Al-Jawher(2022) "A Robust image encryption scheme based on block compressive sensing and Wavelet Transform" Proceeding of 3rd International Conference on Optics, Photonics and Lasers, 20-21 September, 2022 .

[32] Adnan HM Al-Helali, Hamza A Ali, Buthainah Al-Dulaimi, Dhia Alzubaydi, Walid A Mahmoud "Slantlet transform for multispectral image fusion" Journal of Computer Science, Vol.5, Issue 4, PP. 263-267, 2009.

[33] AHM Al-Helali, Waleed A. Mahmoud, HA Ali "A Fast personal palm print authentication Based on 3d-multi Wavelet Transformation", TRANSNATIONAL JOURNAL OF SCIENCE AND TECHNOLOGY, Vol. 2, Issue 8, 2012.

[34] H. Al-Taai, Waleed A. Mahmoud & M. Abdulwahab "New fast method for computing multiwavelet coefficients from 1D up to 3D" , Proc. 1st Int. Conference on Digital Comm. & Comp. App., Jordan, PP. 412-422, 2007.

[35] A H Kattoush, Waleed Ameen Mahmoud Al-Jawher, O Q Al-Thahab "A radon-multiwavelet based OFDM system design and simulation under different channel conditions" Journal of Wireless personal communications, Volume 71, Issue 2, Pages 857-871, 2013.

[36] Waleed A. Mahmoud Al-Jawher, T Abbas – "Feature combination and mapping using multiwavelet transform" IASJ, AL-Rafidain, Issue 19, Pages 13-34, 2006

[37] WA Mahmoud, MS Abdulwahab, HN Al-Taai: "The Determination of 3D Multiwavelet Transform" IJCCCE, vol. 2, issue 4, 2005.

[38] Waleed A Mahmoud Al-Jawher "A Smart Single Matrix Realization of Fast Walidlet Transform" International Journal of Research and Reviews, Vol. 2, Issue 2, PP. 144-150, 2011.

[39] I. Al-Jadir, and Waleed A Mahmoud Al-Jawher "A Grey Wolf Optimizer Feature Selection method and its Effect on the Performance of Document Classification Problem" Journal Port Science Research 4 (2), 116-122

[40] WA Mahmoud, AS Hadi, TM Jawad "Development of a 2-D Wavelet Transform based on Kronecker Product" - Al-Nahrain Journal of Science, Vol. 15, Issue 4, PP. 208-213, 2012