Simultaneous Permutation and Diffusion Based Efficient Chaotic Image Cryptosystem

Biji Babu[1], Annie George[2]
[1]*PG Scholar,* [2]*Assistant Professor*
Dept. of Electronics and communication Engg.
Rajiv Gandhi Institute of Technology Kottayam, India.

***Abstract*—With the developments of communication technologies, sensitive media are processed and delivered in digital format. Most cases this media is imperative and must be maintained from any unauthorized attacks. The security of digital images is very essential for many multimedia applications including military images, medical images systems, wireless networks, and portable devices. To preserve the secretness of the transmitted images, different encryption techniques are employed. In this direction, the chaotic based ciphers have shown brilliant performance. Recently, permutation-diffusion based multimedia encryption techniques have been developed. In traditional architecture, permutation and diffusion functions are applied in two separate phases. This separable design helps the attacker to launch several attacks and also causes to the degradation of the encryption speed. To avoid these problems, in this work, we propose a simultaneous permutation and diffusion-based efficient image cryptosystem which combines pixel scrambling and shuffling using Arnold Cat map, in which the image pixels are processed in a dynamic order fashion. Simulation results, histogram analysis, and key sensitivity analysis proved that the image cipher has several brilliant features and a good performance against various types of attacks. Thus, the cryptosystem is strongly appropriate for practical image security applications.**

***Index Terms*—Encryption, Cipher, Permutation, Diffusion, Arnold Cat map.**

I. Introduction

Multimedia is vital to the digital era, where data transmission has gained much importance. In addition, the rate of insecurity has increased proportionally. This implores the need for various methods to protect data privacy.

Cryptography, steganography, and watermarking are the main methods to protect data privacy. Data protection is the main aim of all of these methods. Out of all these strategies, the chaotic based algorithm tends to satisfy the most asked for features, such as efficiency, security, and safety. Pixel confusion and diffusion are the main principles behind this technique.

The general permutation diffusion based architecture for image encryption is composed of two main building blocks, which are permutation and diffusion operations. The permutation operation only shuffles the positions of the plain image, in order to break the correlation between neighboring pixels of the plain image. While the diffusion operation sequentially changes the pixels values of the permuted plain image by using a quantized chaotic keystream to spread out any slight change of an image pixel to almost all image pixels. Further, the whole architecture is iterated to enhance the encryption effect of the corresponding algorithm.

II. Motivation

Based on the study of several chaotic image cryptosystems with a permutation diffusion structure, it is found that most of the systems carry out the permutation and the diffusion operations as two separate stages. From cryptography view, this separation results in several defects for such architecture. The common defects of these image ciphers are:

a) The initial parameters for the permutation operations are fixed; it will return the same permutation sequence in all permutation-diffusion iterations.
b) For the diffusion stage, the generated keystream is only dependent on the secret initial parameters of the chaos system.

Moreover, the values of image pixels are altered during the diffusion phase in a static fashion from the left upper corner to right bottom corner, which gives significant information about the encryption technique to the attackers. Consequently, an adversary could simply split this architecture into two unrelated stages by feeding the encryption algorithm with a plain image of identical values.

To remedy the mentioned problems, an efficient image encryption technique that combines the permutation and diffusion operation together in one stage is discussed in this paper. Additionally, a dynamical pixel order mechanism for diffusion is also suggested.

III. Literature Review

The different methods used for encrypting images are described.

G. Chen, Y. Mao and C. Chui [1] extended the 2D Cat map to 3D for constructing a secure cryptosystem in which the generalized map is utilized in the permutation phase to scramble the pixels and to mask the shuffled image.

Ji Won Yoon and Hyoungshick Kim [2] proposed a new image encryption algorithm with a large pseudorandom permutation which is computed from chaotic maps combinatorially.

B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi [3] presented a novel algorithm for image encryption based on combining hyper-chaotic sequences and plaintext. The suggested method is a private key encryption system with only one round diffusion process.

J. Chen, Z. Zhu, C. Fu, and H. Yu [4] proposed a fast image encryption scheme with a novel pixel swapping-based confusion strategy. In the proposed confusion strategy, each pixel is swapped with another pixel located after it, and the swapping operation is controlled by a chaotic key stream and the previous pixel.

J. Chen, Z. Zhu, C. Fu, H. Yu, and Y. Zhang [5] presented an efficient image cryptosystem with dynamic reuse of the permutation matrix. Different from the traditional ones, the permutation matrix generated in the confusion phase will be persevered and reused in the diffusion stage.

IV. System Description

This section describes a brief overview of the chaotic systems employed in the image cryptosystem. The Chebyshev-Chebyshev map and the modified Logistic map used in this scheme has several good features compared with a simple seed maps.

a) The distribution of the generated sequence is more uniform than its corresponding simple seed maps.

From the bifurcation diagram, the Logistic map and Chebyshev map [6] have a limited data range within the interval [0, 1]. On the other hand, the produced sequences from the modified Chebyshev- Chebyshev chaotic map and the modified Logistic map spread out in the entire data range of the interval [0, 1].

b) The employed chaotic maps have a wider chaotic range than the corresponding seed maps. This feature can be shown by the Lyapunov exponent as shown in Fig.2.

The Lyapunov exponent of the Chebyshev- Chebyshev chaotic map and the modified Logistic map are always positive in the whole range of the control parameters. On the other hand, the Lyapunov exponents of the seed maps are positive within a limited range of data.

c) Both chaotic maps have better chaotic behavior than their corresponding seed maps.

The Lyapunov exponents of the maps are greater than the corresponding seed maps which indicates the better chaotic behavior.

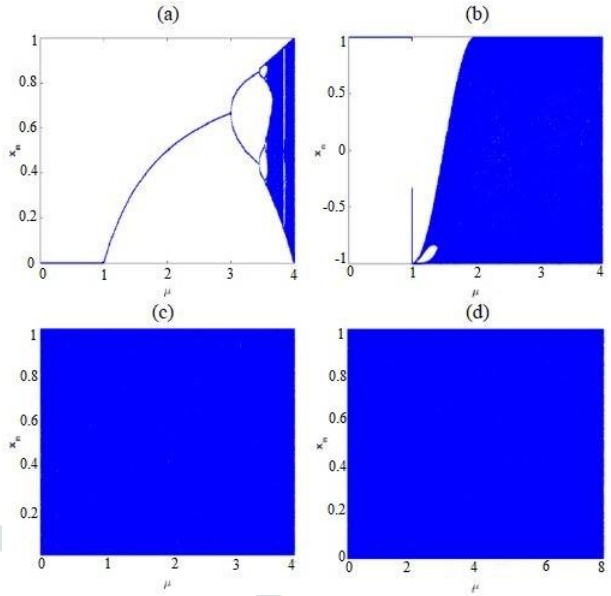

Fig. 1. The Bifurcation diagrams of the (a) Logistic map; (b) Chebyshev map; (c) Modified Logistic map; (d) Chebyshev- Chebyshev map.

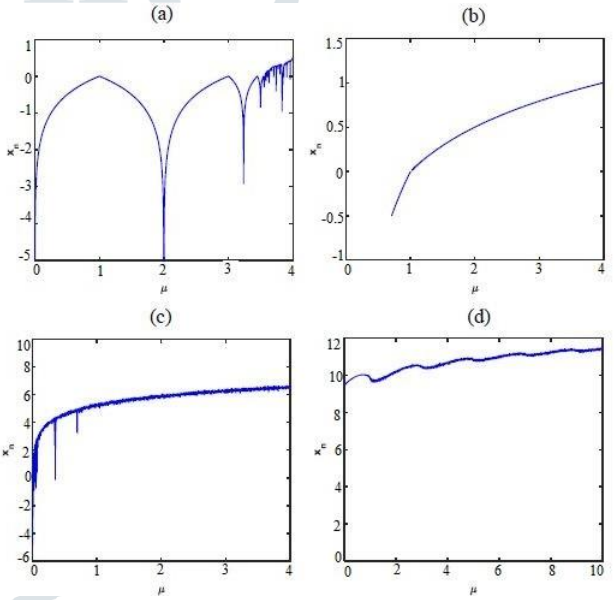

Fig. 2. The Lyapunov Exponent of the (a) Logistic map; (b) Chebyshev map; (c) Modified Logistic map; (d) Chebyshev- Chebyshev map.

A. Image Ciphering Technique

The proposed image ciphering technique [7], [8] uses ten parameters ($x_0, u_1, k_1, N_0, y_0, u_2 \times, k_2, t_0, V_0, V_0'$ and c_0) as a secret key. The scheme consists of five steps:

a) Pixel scrambling using Arnold Cat map
b) Pixel shuffling
c) Generation of intermediate keys
d) Horizontal and vertical mixing
e) Simultaneous permutation and diffusion operations

The Chebyshev-Chebyshev chaotic map is defined as:

$$x_i = cos\,((u_1 + 1) \times \arccos(x_{i-1})) \times 2k_1 - \text{floor}\,(\cos((u_1 + 1) \times \arccos(x_{i-1})) \times 2k_1$$

Where $u_1 \varepsilon$ (0; 10] and $8 < k_1 < 20$ are the control parameters of the Chebyshev-Chebyshev chaotic map and $x_0 \varepsilon$ (0; 1] is an initial parameter for the system.

The modified Logistic map is defined as:

$$y_n = (u_2 \times k_2 \times y_{n-1} \times (1-y_{n-1})) \bmod 1$$

Where $u_2 \varepsilon$ (0; 4] and $k_2 > 1$ are the control parameters of the chaotic map and $y_0 \varepsilon$ (0; 1] is an initial parameter. For the modified Logistic map, the term $u_2 \times k_2$ can be considered as a single parameter with any positive real value which expands the key space of the chaotic map.

1) Pixel Scrambling Using Arnold Cat Map: Arnold Cat map [9] in combination with Chebyshev-Chebyshev chaotic map and the modified logistic map is used to confuse image pixels before encryption, where the positions of the pixels of plain images are shuffled over the whole image without changing the value of the image pixels and the image becomes unrecognizable (Shown in Fig. 4.).

The Arnold Cat chaotic map is defined as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N$$

Where p and q are control parameters of the given map, (N×N) is the dimension of the image, (x_n, y_n) is the pixel location of the plain image, and (x_{n+1}, y_{n+1}) is the pixel location after applying Arnold transformation.

2) Pixel Shuffling: Pixel shuffling is used to add more randomness and to increase the efficiency of the encryption algorithm.

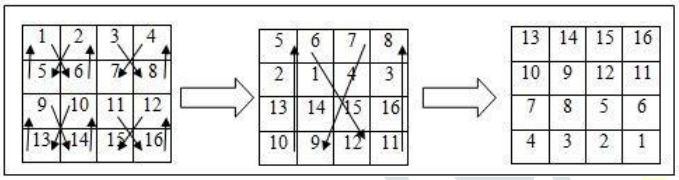

Fig. 3. Pixel Shuffling Algorithm.

The shuffling algorithm represents a secret key for the ciphering technique. The main shuffling steps are:

a) Divide the image into 4 blocks as shown in Fig.3.
b) Each block is shuffled in a predefined order (e.g. the block (1, 2, 5, 6) is shuffled to be (5, 6, 2, 1) as shown in Fig.3.)
c) Step 2 is repeated until it reaches the last quad.
d) Each entire quad is considered as a single cell and shuffled in a predefined order (eg: entire quad (5, 6, 2, 1) is shuffled to be (13, 14, 10, 9) as shown in Fig.3.)

3) Generation of Intermediate Keys: a) Iterate the Chebyshev-Chebyshev chaotic map for N_0+2MN times to get a chaotic sequence for pixel mixing.
N_0, M, and N indicate the secret integer, the width and the height of the plain image respectively.

b) Compute the intermediate keys (key1 and key2) for the pixel mixing.

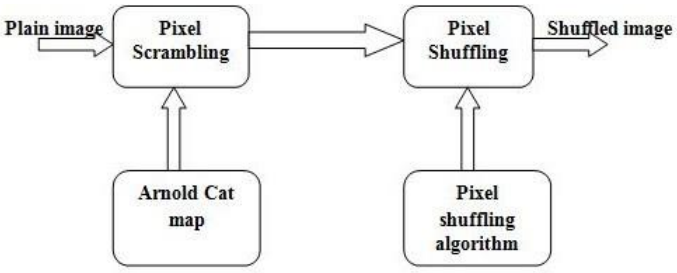

Fig. 4. Pixel Scrambling and Shuffling using Arnold Cat Map.

$$Key_L(i,j) = (x_W \times 10^{14}) \bmod 256$$

Where

$W = N_0 + 2r_1 - 1$ if $L = 1$

$N_0 + 2r_2$ if $L = 2$

Where r_1 and $r_2 = 1, 2, \ldots\ldots, MN$

The first key stream is obtained from the values indexed by the odd position in the chaotic sequence x, while keystream2 is obtained by the even indices.

4) Horizontal and Vertical Mixing of Image Pixels: To mix the plain image pixels information, sequentially chaining them through XOR operation. Horizontal pixel mixing is applied row-wise from the first image pixel to the last one to make each pixel of the plain image influenced by all preceding pixels of that image. Similarly, the vertical pixel mixing is applied in column-wise in reverse order from the last image pixel to the first one.

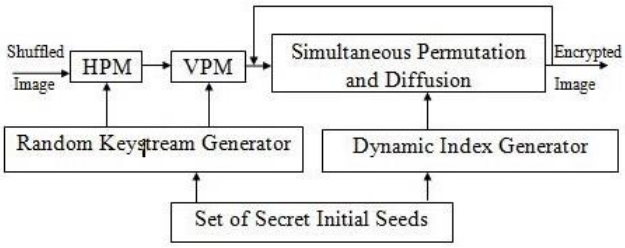

Fig. 5. Architecture for image ciphering.

5) The Simultaneous Permutation and Diffusion Operation:
a) Iterate the modified Logistic map t_j times using the initial parameter y_j.

$$y_j = (y_0 + (c_{sj} \div 255)) \bmod 1$$

$$t_j = t_0 + c_{sj}$$

Where y_0 and t_0 are initial seeds and they are part of the secret key. The value of sj is determined at each step according to:

$$s_j = \begin{cases} 0 & \text{if } j = 1 \\ MN & \text{if } j = 2 \\ s_{j-1} - 1 & \text{otherwise} \end{cases}$$

Both the initial value and the number of iterations of the chaotic map at each step of the ciphering is not fixed and it is severely correlated to the previously encrypted pixel along with the secret parameters of the chaotic map. In particular, the ciphering technique generates a distinct key stream and can be exploited to generate a dynamical pixel order for each different image while the secret parameters maintain the secrecy.

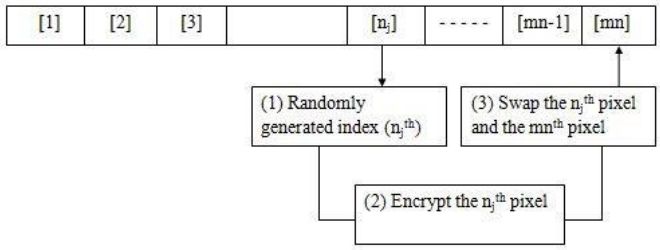

Fig. 6. The depiction of simultaneous permutation and diffusion.

b) Calculate the value of n_j to determine the index of the processed pixel according to:

$$n_j = | y_{tj} \times 10^{14} | \bmod s_{j+1} + 1$$

This chaotically generates a dynamical order model by which the pixels are encrypted and permuted. Specifically, it generates a random value n_j ranging from 1 to MN to randomly select a pixel from the plain image.

c) Compute the key-stream for encryption associated to the processed pixel according to:

$$\varphi j = | y_{tj} \times 10^{14} | \bmod 256$$

d) Encrypt the n_j th pixel of the image based on the equation:

$$c_{nj} = (c_{nj} + \varphi_j) \bmod 256 \text{ XOR } c_{sj}$$

c_{sj} is the previous swapped-ciphered pixel

e) Swap the encrypted pixel

This algorithm enables the cipher to randomly choose one of the non-encrypted pixels of the plain image at each step of the algorithm. On the other hand, according to the symmetric nature of the image cipher, the decryption process can correctly retrieve the plain-image by reversing the order of the steps of the encryption using the same secret key.

Swap the ciphered pixel c_{nj} and pixel c_{sj+1}according to:

$$\text{Temp} = c_{nj} \text{ , } c_{nj} = c_{sj+1} \text{ , } c_{sj+1} = \text{Temp}$$

V. Results & Analysis

This section is discussed about the simulation results and security analysis for the suggested cipher to demonstrate its validity and effectiveness. The results and analysis of only four gray-scale plain images (Barbara, Goldhill, Pepper, and Tank).

A. Scheme Effectiveness Evaluation of Image Cipher

Fig.7. represents the modified ciphering technique that uses Arnold Cat map in combination with the normal ciphering method. Here the input plain image is scrambled four times using Arnold map. After that, the scrambled image is shuffled over the entire image pixels by using a predefined pixel shuffling algorithm. Then the shuffled images are encrypted using the simultaneous permutation diffusion method.

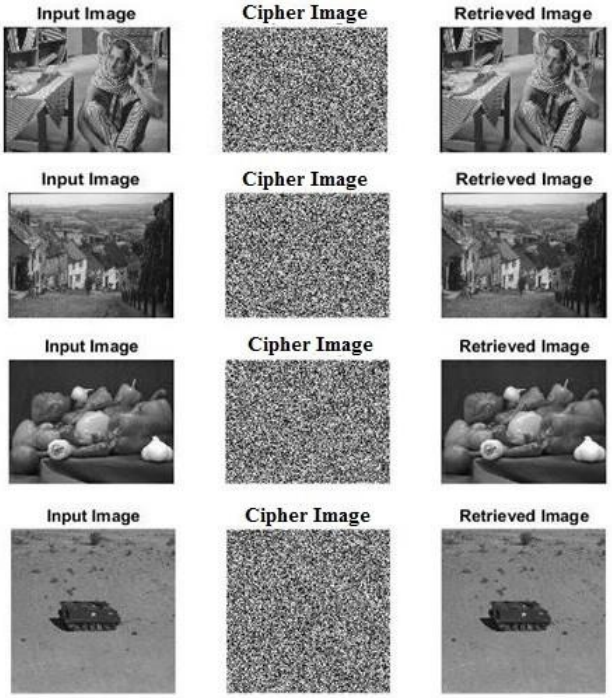

Fig. 7. Encryption and decryption proposed algorithm.

B. Histogram Analysis Of Image Cipher

An image histogram shows the distribution of the values of an image. The histogram for the plain-images and the associated encrypted ones are displayed in Fig.8.

The histogram for the encrypted images is closely uniform distributed and varies from that of the plain-images. Accordingly, no information about the plain images can be extracted from their enciphered images, which in turn, makes the statistical attack totally infeasible.

C. Key sensitivity test of image cipher

A robust image cipher must be sensitive to slight changes in the encryption keys. Any secure enciphering algorithm must produce completely different cipher images for a single bit variation in the encryption keys.

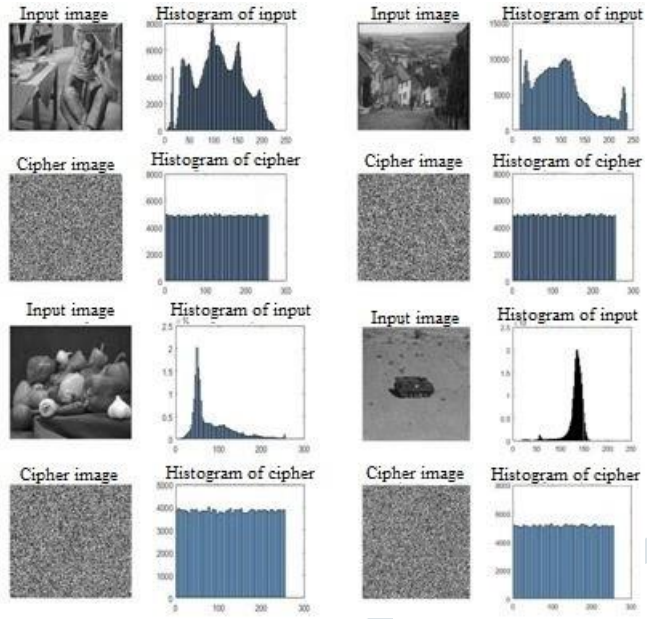

Fig. 8. Histogram analysis of the image.

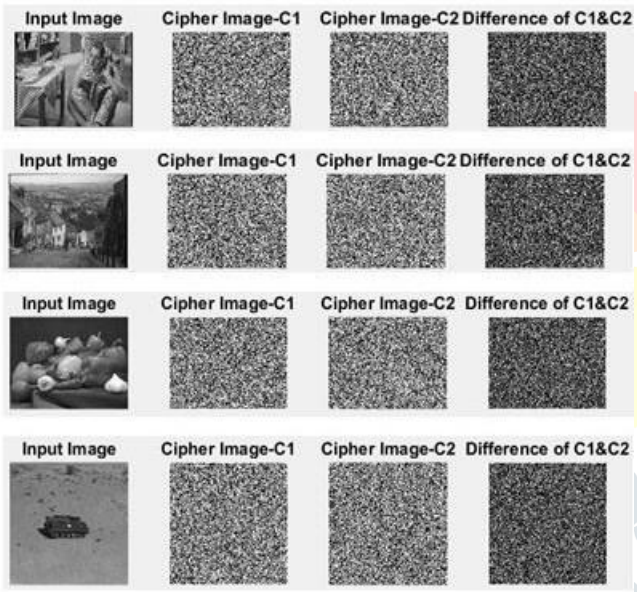

Fig. 9. The results of key sensitivity for the cryptosystem.

To estimate the key sensibility, a set of initial seeds and control parameters are chosen. After this, the plain image P is encrypted using these values to get the enciphered image C1. Then, a tiny change is made to any of the secret key parameters and the image P is enciphered again to obtain another cipher image C2.

D. Signal to Noise Ratio Comparison

This subsection calculates the signal to noise ratio of the ciphering algorithm. Fig.10. represents the SNR image of the proposed ciphering method. The suggested method adds more randomness and confusions to the plain image before encryption.

Fig. 10. SNR image of the proposed cipher.

E. Comparison of Input Image and Retrieved image

The intensity plot of both input and retrieved images in Fig.11. are same, the SSIM value is equal to one and the correlation coefficients in Table I for both input and retrieved images are the same, which indicates the retrieved image is entirely identical to the corresponding input plain images.

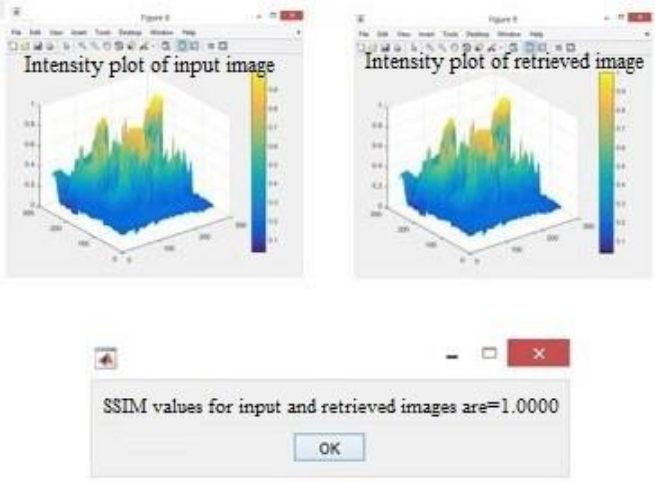

Fig. 11. Intensity Plots.

Test Images	Correlation Coefficients					
	Original Image			Retrieved Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Pepper	0.9810	0.9783	0.9630	0.9810	0.9783	0.9630
Barbara	0.9079	0.9489	0.8659	0.9079	0.9489	0.8659
Goldhill	0.9711	0.9740	0.9508	0.9711	0.9740	0.9508
Tank	0.9637	0.9343	0.9228	0.9637	0.9343	0.9228

TABLE I
CORRELATION COEFFICIENTS OF ORIGINAL AND RETRIEVED IMAGES

Test Images	Proposed Ciphering Technique			
	PSNR	SSIM	NPCR (%)	UACI (%)
Pepper	8.3071	0.0082	99.61	31.74
Barbara	11.640	0.0092	99.64	29.10
Goldhill	10.376	0.0076	99.63	31.03
Tank	17.726	0.0110	99.63	25.95

TABLE II
PSNR, SSIM, NPCR AND UACI ANALYSIS

F. Differential Attack Analysis

NPCR (Number of Pixels change Rate) indicates the number of pixels change rate in the ciphered image while one pixel of the plain image changed. Also UACI (Unified Average Changing Intensity) calculates the average intensity of differences between the plain input image and ciphered image. The ideal value for NPCR and UACI are 100 % and 33.33 % respectively. When the value of NPCR gets closer to 100 %, the ciphering algorithm is more sensitive to the changing of the plain input image, therefore the algorithm can effectively prevent plaintext attack. Also when the value of UACI gets closer to 33.33 %, the algorithm can effectively prevent the differential attack. (Analysis is shown in Table II)

Peak Signal-to-Noise Ratio (PSNR) calculates the estimates of the quality of ciphered image compared with an original input image and is a standard way to measure image fidelity.

G. Correlation analysis

An effective encryption algorithm must eliminate or reduce the strong relationship between adjacent pixels in the enciphered image. The correlations between two horizontally, vertically and diagonally adjacent pixels in the encrypted images shown in TableIII. From these computational results, we found that the cipher algorithm offers the smallest average correlation value between the adjacent pixels of the encrypted images, which is a good indicator for the superior performance of the cipher against various types of attacks.

Test Images	Correlation Coefficients		
	Horizontal	Vertical	Diagonal
Pepper	0.0023	0.0014	0.0017
Barbara	0.0011	0.0042	0.0079
Goldhill	0.0052	0.0032	0.0094
Tank	0.0038	0.0027	0.0061

TABLE III
CORRELATION COEFFICIENTS OF CIPHER IMAGES

FUTURE ENHANCEMENT

Currently, the chaos-based encryption scheme was designed for still images and moving images. The popularity of this ciphering technology in the society has promoted digital images and videos to play an important role than the traditional texts, which appeals the honest protection of users privacy. To accomplish such security and privacy requirements in multi-media applications, encryption of images and videos is very necessary to discourage malicious attacks from unauthorized parties. Hence we can extend this thesis work to design a permutation-diffusion encryption scheme for moving images (videos). We can also improve security as well as execution time for this ciphering scheme.

CONCLUSION

Most of the cryptosystem carry out the permutation and the diffusion processes as two separate stages. This separation causes several defects for such architecture. Thus, in most cases, the attacker can break such schemes by launching known or chosen plaintext attacks. But an efficient technique that combines permutation and diffusion operation together in one stage is discussed here. These operations processed the image pixels in a dynamic order. This technique employed an Arnold Cat map to scramble and shuffle the image pixels to add more randomness and confusions and also the Chebyshev-Chebyshev chaotic map and the modified Logistic chaotic map is used to implement this structure. Simulation results, histogram analysis, and key sensitivity analysis proved that the image cipher has several brilliant features and a good performance against various types of attacks. Thus, the cryptosystem is strongly appropriate for practical image security applications.

REFERENCES

[1]G. Chen, Y. Mao, and C. Chui,"A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons Fractals., vol. 21, no. 3, pp. 749-761, 2004.

[2]Ji Won Yoon, and Hyoungshick Kim,"An image encryption scheme with a pseudorandom permutation based on chaotic maps," Commun Nonlinear Sci Numer Simulator., pp. 3998-4006, 2010.

[3]B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi,"A simple, sensitive and secure image encryption algorithm based on hyperchaotic system with only one round diffusion process," Multimed. Tools Appl., vol. 71, no. 3, pp. 1469-1497, 2014.

[4]J. Chen, Z. Zhu, C. Fu, and H. Yu,"A fast image encryption scheme with a novel pixel swapping based confusion approach," Nonlinear Dyn., vol.77, no. 4, pp. 1191-1207, 2014.

[5]J. Chen, Z. Zhu, C. Fu, H. Yu, and Y. Zhang, "Reusing the permutation matrix dynamically for efficient image cryptographic algorithm," Signal Process., vol. 111, pp. 294-307, 2015.

[6]S. El Assad, and M. Farajallah, A new chaos-based image encryption system, Signal Processing: Image Communication, vol. 41, pp. 144-157, 2016.

[7]Y.P. Li, C.H. Wang, and H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Optics and Lasers in Engineering, vol. 90, pp. 238-246, 2017.

[8]Hossam Diab, "An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations," Digital Object Identifier, 10.1109/ACCESS.2017.

[9]Hikmat N. Abdullah, Hamsa A. Abdullah, "Image encryption hybrid chaotic map," Information Technology, 2017.