DWT AND HASH FUNCTION BASED NOVEL IMAGE ENCRYPTION

S. Praveena
ECE Dept, M.G.I.T,Hyderabad

Abstract: this paper proposed a new image encryption framework based on the Discrete Wavelet Transform, Arnold Transform. Here the proposed approach accomplished the DWT which represents the image in the frequency domain by which the attacker can't acquire the information easily. Further similar to the existing approach the control parameters of the cat map, i.e. the permutation key, are determined by the Murmur2 hash value of the original image. This approach Provides more security to the image information. This also achieves Maximum similarities in the entropies of original and encrypted image.

Keywords: Image Encryption, DWT, Arnold Cat Map, MurmurHash2, Lorenz, Entropy, Correlation.

I. INTRODUCTION

The end of the 20th century was marked by an extraordinary technical revolution from analog to numerical as documents and equipment became increasingly used in various domains. However, the advantages of the digital revolution were not achieved without drawbacks such as illegal copying and distribution of digital multimedia documents. To meet this challenge, researchers were motivated more than ever to protect multimedia documents with new and efficient document protection techniques. In this context, different techniques have been introduced such as encryption and digital watermarking. The first one consists in transforming multimedia documents using an algorithm to make it unreadable to anyone except for the legitimate users. The second one consists of embedding digital watermarks into multimedia documents to guarantee the ownership and the integrity of the digital multimedia contents. The protection of images is of particular interest in this paper. Traditional image encryption algorithms such as private key encryption standards (DES and AES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC), as well as the international data encryption algorithm (IDEA), may not be the most desirable candidates for image encryption, especially for fast and real-time communication applications. In recent years, several encryption schemes have been proposed [1–12]. These encryption schemes can be classified into different categories such as value transformation [1–4], pixels position permutation [5–8], and chaotic systems [9–12]. Existing approach presents a new chaos-based image cipher using a plaintext-related permutation. The cat map and Lorenz system are employed to shuffle the positions of image pixels and generate the diffusion key stream, respectively. The control parameters of the cat map, i.e. the permutation key, are determined by the Murmur2 hash value of the original image. Owing to the avalanche property of hash functions, completely different shuffled images will be produced even if there is a tiny difference between the original ones, and it helps accelerate the diffusion process. However they are less secure. The entire process of encryption is carried out in the spatial domain. The attacker can hack acquire the information from the encrypted image easily. More complexity due to the two transformations, one at pixel position level and another at pixel value level. Much deviation in the entropies of original and encrypted images.

To overcome the drawbacks with the existing approach this approach proposed a new image encryption framework based on the Discrete Wavelet Transform, Arnold Transform. Here the proposed approach accomplished the DWT which represents the image in the frequency domain by which the attacker can't acquire the information easily. Further similar to the existing approach the control parameters of the cat map, i.e. the permutation key, are determined by the Murmur2 hash value of the original image. This approach Provides more security to the image information. This also achieves Maximum similarities in the entropies of original and encrypted image. Rest of the paper is organized as follows: section II illustrates the literature survey details. Section III describes the details of proposed approach. The simulation results are described in section IV and section V concludes the paper.

II. RELATED WORK

In 2008 Mohammad Ali Bani Younes and Aman Jantan [13] proposed a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. In 2008 Mohammad Ali Bani Younes and Aman Jantan [14] introduced a new permutation technique based on the combination of image permutation followed by encryption I.e. well known encryption algorithm called RijnDael. Amitava Nag et.al. [15] Proposed a two phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation in year 2011. With the help of four 8-bit key applied, the pixel values are redistributed on different location using affine transform technique. Yicong Zhou and Sos Agaian [16] introduce a new method of applying the image steganography concept for image encryption. They used the concept of e PLIP (Parameterized Logarithmic Image Processing) addition to embed the scrambled original image into a selected cover image, it generates an encrypted image. In 2011 Yun sen and Gunayi Wang [17] proposed a modified chaotic map technique In order to improve the security of chaotic encryption algorithm. One of the advantage of their technique is that when we compared it with original logistic map, their proposed map makes it always be chaotic, and expands the iteration range from original (0, 1) to (0, 4λ) (λ>0.25).

In 2012 Qiudong Sun et.al. [18] Presented a random scrambling algorithm based on bit-planes decomposition of image. Their Algorithm starts by decomposing a gray image into bit-plane images, each image for separate bit plane. In the next step every bit plane image is shuffled by using a random scrambling algorithm. At last, all the shuffled bit plane images are merged according to their original levels on bit-planes and we obtained an encrypted image. In 2012 Sukalyan Som and Atanu Kotal [19] presented multiple chaotic maps based a new symmetric image encryption algorithm. In the proposed algorithm, with the help of generalized Arnold Cat Map, the plain image is first scrambled. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one dimensional Logistic Map after preprocessing them to integers. In 2013 A.Kester [20] proposed a new technique that contribute to the general body of knowledge in the area of cryptography application by developing a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values.

In [21], the feasibility of selective image encryption on a bitplane is investigated. It is concluded that only selectively encrypting 50% of the whole image data can gain an acceptable security. Therefore, the encryption time is substantially reduced. In [22-25], schemes with certain diffusion effect introduced in the permutation stage are proposed. As the pixel value mixing effect is contributed by both stages, the number of iteration rounds required by the diffusion procedure is reduced, and hence the performance of the cryptosystem is improved.

III PROPOSED APPROACH

A new chaos-based image cipher using cat map and Lorenz system through Discrete Wavelet Transform is suggested in this chapter. The control parameters of the cat map are determined by the Murmur2 hash value of the original image. Owing to the avalanche property of hash functions, completely different shuffled images will be produced even if there is a tiny difference between the original ones. The architecture of the proposed scheme is illustrated by Fig.1.

Under this structure, the original image is firstly decomposed through Discrete Wavelet transform into subbands. All the obtained frequency bands are formulated into a band scrambling matric by the horizontal followed by vertical concatenation. Then the Band scrambling matrix is shuffled by using Arnold cat map, whose control parameters, i.e. the permutation key, are given by the hash value of the original image. As is known, the essential property of a hash function is that it almost surely produces different hash values for different messages. This means different images are rearranged in different ways and a satisfactory diffusion effect will be achieved with only one round of encryption.

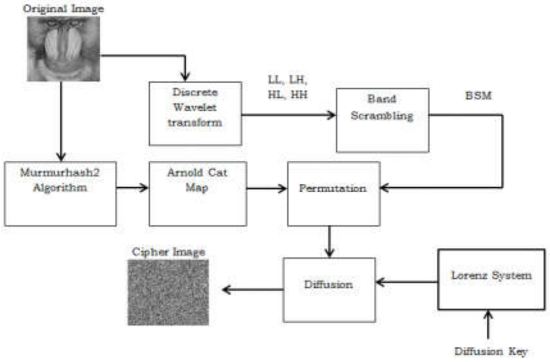


Figure.1 Architecture or proposed image encryption model

In our scheme, the 64-bit version Murmurhash2 algorithm, created by Austin Appleby in 2008, is employed. The algorithm outperforms most other ones because of its excellent distribution, avalanche behavior, collision resistance and performance. In the diffusion stage, the shuffled data are masked by a key stream extracted from the orbit of Lorenz system. A large key space is ensured as the three state variables of the Lorenz system are used as the diffusion key. The detailed DWT, permutation and diffusion operations are discussed as follows.

A. Permutation Process

The Arnold cat map, described by Eq. (1), is a chaotic bijection of a unit square onto itself.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ 1 \quad (1)$$

Where *p* and *q* are control parameters, and *x* mod 1 means the fractional part of *x* for any real number *x*. To incorporate the map into image permutation that operated on a lattice of finite number of pixels, it has to be discretized. This can be done simply by changing the range of (*x*, *y*) from the unit square to the lattice *N*×*N*, as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (2)$$

Where *N* is the number of pixels in one row (column). The inverse transform of the map is easily found to be given by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (3)$$

To determine the value of *p* and *q*, the 64-bit Murmur2 hash value of the original image is firstly divided into two 32- bit parts, which are denoted by *hashl* and *hashr*, respectively. As the four-tuple [1, (*p*+*k*1*N*), (*q*+*k*2*N*), (*p*+*k*3*N*)(*q*+*k*4*N*)+1] produce the same output as the four-tuple [1, *p*, *q*, (*pq*+1)] for any *k*1, *k*2, *k*3, *k*4∈*Z*, the two parameters are given by *mod*(*hashl*, *N*) and *mod*(*hashr*, *N*), respectively. The utilization of small parameters also speeds up the calculation. The pseudo code of the MrumurHash2 algorithm is listed below, where the argument *key* is a pointer that points to the image data. As can be seen from the pseudo code, the algorithm uses bitwise and integer multiplication operations to manipulate and update the hash value. As is known, the two operations are very efficient for hardware implementation, and thereby the computation cost of the hash algorithm is much lower than that of one round of diffusion operation, where the manipulations of real numbers are required.

MurmurHash is a non-cryptographic hash function suitable for general hash-based lookup. It was created by Austin Appleby in 2008 and is currently hosted on Github along with its test suite named 'SMHasher'. It also exists in a number of variants, all of which have been released into the public domain. The name comes from two basic operations, multiply (MU) and rotate (R), used in its inner loop. Unlike cryptographic hash functions, it is not specifically designed to be difficult to reverse by an adversary, making it unsuitable for cryptographic purposes.

B. Diffusion Process

The well-known Lorenz system, developed by Edward Lorenz in 1963 for atmospheric convection, is described by

$$\begin{cases} \dot{x} = \sigma(y-x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \quad (4)$$

where *t* is time and σ, ρ, β are the system parameters. The system is chaotic for the values of σ =10, ρ =8/3, β=28. The initial values of the state variables, (*x*0, *y*0, *z*0), are used as the diffusion key.

The detailed diffusion process is described as follows:

Step 1: Arrange the pixels of the shuffled image to a vector *p*={p_0, p_1, …, $p_{N\times N-1}$} in the order from left to right, top to bottom.

Step 2: Generate a keystream with length equal to *p*.

Step 2.1: Pre-iterate system (4) for I_0 times to the harmful effect of transitional procedure, where *I*0 is a constant. The fourth-order Runge-Kutta method is employed for solving the equation.

Step 2.2: Iterate system (4) for *t* times, where *t* =ceil(*N*×*N*/3). For each iteration, the current values of the three state variables are appended to a vector *Ls*={s_0, s_1, …, $s_{N\times N-1}$}. Obviously, there are *r* = (*t*×3-*N*×*N*) redundant elements, which are discarded.

Step 2.3: Qualify a keystream *k*={k_0, k_1, …, $k_{N\times N-1}$} from *Ls* according to

$$k_n = mod\left[sig_{N(abs(s_n))}, 2^L\right] \quad (5)$$

Where *L* is the color depth of the original image, *abs*(*x*) returns the absolute value of *x*, and *sig_n*(*x*) returns the *n* most significant decimal digits of *x*, where *n* is the precision of *x*. In our scheme, all the variables are declared as double-precision type, which has a precision of 15 decimal digits.

Step 3: Calculate the cipher-pixels value according to Eq.(4.6).

$$c_n = k_n \oplus \{[p_n + k_n] mod\ 2^L\} \oplus c_{n-1} \quad (6)$$

where c_n and c_{n-1} are the output and previous cipher-pixels, respectively, and $\oplus$ performs bit-wise exclusive OR operation. One may set the initial value *c*_1 as a constant. The decipher procedure is the same as that of the encipher process described above except that the inverse of Eq. (6), described by Eq. (7), is employed.

$$p_n = [k_n \oplus c_n \oplus c_{n-1} + 2^L - k_n] mod\ 2^L \quad (7)$$

IV. SIMULATION RESULTS

To evaluate the effectiveness of the proposed permutation method, various test images are processed through the proposed image encryption approach and the performance is evaluated through the performance metrics such as entropy, correlation, NPCR and UACI. The mathematical formulation for the above metrics is as follows;

$$H(X) = -\sum_{i=1}^{N} P(x_i)\log\left(P(x_i)\right) \quad (8)$$

Where *X* is a random variable with *N* outcomes {x_1, ..., x_N} and $P(x_i)$is the probability mass function of outcome *xi*.

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i-\bar{y})^2\right)}} \quad (9)$$

$$\bar{x} = \sum_{i=1}^{N} x_i \qquad (9)$$

$$\bar{y} = \sum_{i=1}^{N} y_i \qquad (10)$$

Where x_i and y_i are grayscale values of the *i*th pair of adjacent pixels, and *N* denotes the total number of samples.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{W \times H} \times 100\% \qquad (11)$$

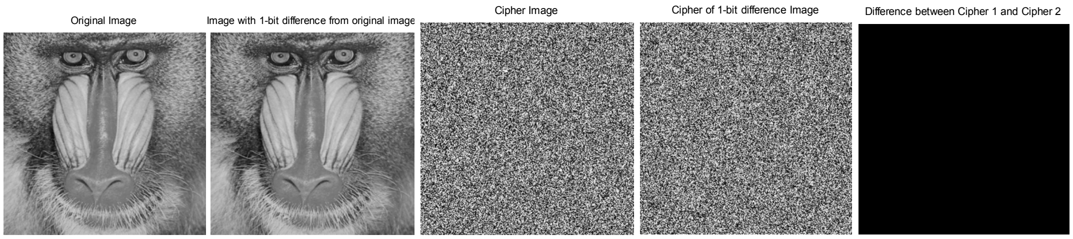
$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|P_1(i,j) - P_2(i,j)|}{L-1}\right] \times 100\%$$

(12)

Where *W* and *H* are the width and height of P_1 or P_2 and $D(i, j)$ is defined as

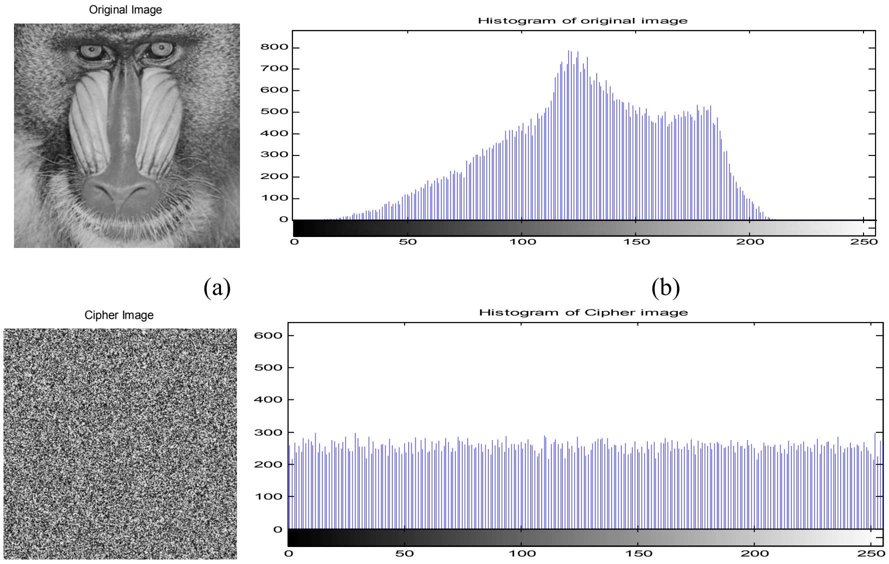
$$D(i,j) = \begin{cases} 0 \ if \ P_1(i,j) = P_2(i,j) \\ 1 \ if \ P_1(i,j) \neq P_2(i,j) \end{cases} \qquad (13)$$

The sample test images considered for evaluation are represented in figure.3 and the obtained results are shown in figure 2 and figure.3.


Original Image
Image with 1-bit difference from original image
Cipher Image
Cipher of 1-bit difference Image
Difference between Cipher 1 and Cipher 2

(a) (b) (c) (d) (e)

Fig.2. The application of the proposed permutation algorithm. (a) the original Baboon test image; (b) the image with 1-bit difference from (a); (c) the shuffled image corresponding to (a); (d) the shuffled image corresponding to (b); (e) the differential image between (c) and (d).



(a) (b)

(c) (d)

Fig.3. Histograms of the Baboon test image and its output cipher image. (a) The Baboon test image; (b) histogram of (a); (c) cipher image corresponding to (a); (d) histogram of (c).

The obtained entropies of all above test images are represented in table.1.

Table.1 entropies of original and cipher images

Test Image	**Entropy**	
	Plain Image	**Cipher Image**
Peppers	7.5721	7.9969
Lena	7.4366	7.9970
Barbara	7.4838	7.9973
House	7.2743	7.9975
Baboon	7.2283	7.9970
Bus	7.5209	7.9973
Dinosaur	4.3768	7.9968
Elephant	7.2498	7.9970

Rose	7.4488	7.9974
Horse	6.9544	7.9972

Table.2 Correlation Coefficients for Adjacent Pixels in Five Test Images and Their Output Cipher Images

Test Image	**Original**			**Ciphered**		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Peppers	0.9654	0.9679	0.9142	-0.0034	-0.0030	-0.0997
Lena	0.9492	0.9744	0.9363	-0.0042	0.0021	0.0117
Barbara	0.9022	0.9485	0.9260	-0.0095	-0.0073	-0.0257
House	0.8952	0.8994	0.8403	0.0074	-0.0058	0.0653
Baboon	0.8742	0.8219	0.7549	0.0058	-0.0029	0.0178
Bus	0.9028	0.8847	0.7966	0.0030	-0.0060	-0.0101
Dinosaur	0.9624	0.9684	0.9863	0.0011	0.0005	-0.0027
Elephant	0.9084	0.9530	0.8880	0.0022	-0.0017	-0.0145
Rose	0.9890	0.9885	0.9849	0.0055	0.0011	0.0306
Horse	0.8504	0.9100	0.8252	0.0025	-0.0023	-0.0517

V. CONCLUSION

This paper proposed a new DWT and chaos-based image cipher using a plaintext-related permutation. The cat map and Lorenz system are employed to shuffle the positions of image pixels and generate the diffusion key stream, respectively. The control parameters of the cat map, i.e. the permutation key, are determined by the Murmur2 hash value of the original image. Owing to the avalanche property of hash functions, completely different shuffled images will be produced even if there is a tiny difference between the original ones, and it helps accelerate the diffusion process. Experimental results indicate that the proposed scheme requires only one and two cipher cycles to achieve acceptable and satisfactory diffusion properties, respectively, whereas two and three cipher cycles are needed by typical schemes to achieve the same properties. Thorough security analysis is carried out, and the results demonstrate the satisfactory security of the proposed scheme.

REFERENCES

[1] Z. Liu, L. Xu, C. Lin, J. Dai, and S. Liu, “Image encryption scheme by using iterative random phase encoding in gyrator transform domains,” *Optics and Lasers in Engineering*, vol. 49, no. 4, pp. 542–546, 2011.

[2] Q. Guo, Z. Liu, and S. Liu, “Color image encryption by using Arnold and discrete fractional random transforms in HIS space,” *Optics and Lasers in Engineering*, vol. 48, no. 12, pp. 1174–1181, 2010.

[3] Z. Liu, H. Chen, T. Liu et al., “Image encryption by using gyrator transform and Arnold transform,” *Journal of Electronic Imaging*, vol. 2, no. 4, pp. 345–351, 1993.

[4] R. Tao, X. Y. Meng, and Y.Wang, “Image encryption with multi-orders of fractional Fourier transforms,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 734–738, 2010.

[5] R. Zunino, “Fractal circuit layout for spatial de-correlation of images,” *Electronics Letters*, vol. 34, no. 20, pp. 1929–1930, 1998.

[6] G. Zhang and Q. Liu, “A novel image encryption method based on total shuffling scheme,” *Optics Communications*, vol. 284, no. 12, pp. 2775–2780, 2011.

[7] X.-Y. Zhao and G. Chen, “Ergodic matrix in image encryption,” in *Proceedings of the 2nd International Conference on Image and Graphics*, vol. 4875, pp. 394–401, August 2002.

[8] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, “A chaosbased symmetric image encryption scheme using a bit-level permutation,” *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[9] C. K. Huang and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” *Optics Communications*, vol. 282, no. 11, pp. 2123–2127, 2009.

[10] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[11] X. Y. Wang, L. Yang, R. Liu, and A. Kadir, “A chaotic image encryption algorithm based on perceptron model,” *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[12] Y. Wang, K. W. Wong, X. Liao, and G. Chen, “A new chaos-based fast image encryption algorithm,” *Applied Soft Computing Journal*, vol. 11, no. 1, pp. 514–522, 2011.

[13] Mohammad Ali Bani Younes and Aman Jantan,” Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03,2006.

[14] Mohammad Ali Bani Younes and Aman Jantan ,”an image encryption Approach using a combination of permutation technique followed by Encryption”, International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[15] Amitava Nag, “Image Encryption Using Affine Transform and XOR Operation”, IEEE International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011.

[16] Yicong Zhou, Sos Agaian,” Image Encryption Using the Image Steganography Concept and PLIP Model”, Proceedings of 2011 International Conference on System Science and Engineering, Macau, China - June 2011.

[17] Yue Sun, Guangyi Wang,” An Image Encryption Scheme Based on Modified Logistic Map”, Fourth International Workshop on Chaos-Fractals Theories and Applications, 2011.

[18] Qiudong Sun, “Image Encryption Based on Bit-plane Decomposition and Random Scrambling”, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012 .

[19] Sukalyan Som, Atanu Kotal,” Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps”, National Conference on Computing and Communication Systems (NCCCS), 2012.

[20] Quist-Aphetsi Kester,” A cryptographic Image Encryption technique based on the RGB PIXEL shuffling”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, January 2013.

[21] T. Xiang, K. W. Wong, and X. Liao, “Selective image encryption using a spatiotemporal chaotic system,” Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 17, no. 2, article no. 023115, 2007.

[22] K. W. Wong, B. S. H. Kwok, and W. S. Law, “A fast image encryption scheme based on chaotic standard map,” Physics Letters A, vol. 372, no.15, pp. 2645-2652, 2008.

[23] C. Fu, B. B. Lin, Y. S. Miao, X. Liu, and J. J. Chen, “A novel chaos based bit-level permutation scheme for digital image encryption,” Optics Communications, vol. 284, no. 23, pp. 5415-5423, 2011.

[24] C. Fu, W. H. Meng, Y. F. Zhan, Z. L. Zhu, F. C. Lau, K. T. Chi, and H. F. Ma, “An efficient and secure medical image protection scheme based on chaotic maps,” Computers in biology and medicine, vol. 43, no. 8, pp. 1000-1010, 2013.

[25] C. Fu, J. B. Huang, N. N. Wang, Q. B. Hou, and W. M. Lei, “A symmetric chaos-based image cipher with an improved bit-level permutation strategy,” Entropy, vol. 16, no. 2, pp. 770-788, 2014.

[26] K. W. Wong, B. S. H. Kwok, and C. H. Yuen, “An efficient diffusion approach for chaos-based image encryption,” Chaos, Solitons & Fractals, vol. 41, no. 5, pp. 2652-2663, 2009.

[27] Y. Wang, K. W. Wong, X. Liao, and G. Chen, “A new chaos-based fast image encryption algorithm,” Applied soft computing, vol. 11, no. 1, pp. 514-522, 2011.

[28] C. Fu, J. J. Chen, H. Zou, W. H. Meng, Y. F. Zhan, and Y. W. Yu, “A chaos-based digital image encryption scheme with an improved diffusion strategy,” Optics Express, vol. 20, no. 3, pp. 2363-2378, 2012.