A Robust Image Encryption Method Based on Bit Plane Decomposition and Multiple Chaotic Maps

W. Auyporn and S. Vongpradhip
Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand
Email: Wipawadee.a@student.chula.ac.th, Sartid@cp.eng.chula.ac.th

***Abstract*—Multimedia security is very important for multimedia communications over open network. For some applications, the highly robust image encryption approach is needed. This project aims to design a high security image encryption method, since the conventional encryption methods such as DES, AES, and RSA do not suit for image data because there are high correlations and redundancy among pixels in natural images. By using two concepts; bit plane decomposition and multiple chaotic maps, the proposed encryption scheme offers more robust encryption method that is suitable for image data. In the confusion stage of the encryption, the image data is decomposed into eight bit planes, and then each bit plane is permuted separately based on different chaotic map. After that, eight bit planes are recomposed and performed XOR operation with a generated random bit matrix in order to alter all pixel values completely. In diffusion stage, the image is diffused based on a new generated sequence, and performed XOR operation again with another random bit matrix before iterating the diffusion process. The performance of the proposed method is evaluated by using statistical, key space, and key sensitivity analysis. The results show that the proposed image encryption method is very secure and robust against different attacks.**

***Index Terms*—image encryption, chaotic maps, confusion-diffusion type, image processing for security**

I. Introduction

Due to the rapid growth in communications technology, digital contents have been used in many applications such as medical, industrial, or even military applications. The digital data is easy to be intercepted by non-recipients over unsecure networks. Therefore, it is very crucial to hide the multimedia content for transmission. One technique to protect data privacy is cryptography. The basic structure of a cryptographic system is shown in Fig. 1. Encryption is the process to convert the readable information or plain-text/plain-image to non-readable data or cipher text/cipher image. Only receivers with the secret key can decrypt the cipher data and read the content. However, the traditional encryption algorithms such as data encryption standard (DES), advanced encryption standard (AES), and RSA only work well with plain text, but do not suit for image data, because in natural images, adjacent pixels are highly correlated and redundant [1]. Therefore, more complex algorithm to encrypt the image data is needed.

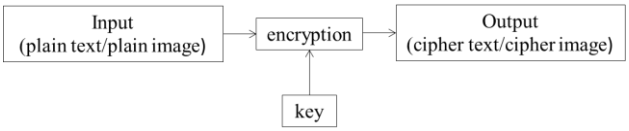


Figure 1. Basic structure of a cryptographic system

Chaos-Based techniques have been extensively studied in the recent years, because their properties lead to the potential cryptography [2]-[7]. There are meaningful relationship between chaos and cryptography. The chaotic system has the properties of ergodicity and sensitivity to initial conditions. In the same way, the good cryptographic system also needs the properties of confusion and diffusion with tiny change in plaintext/plain image or secret key [8]. Both systems are deterministic dynamics, which create random-like behaviors. The chaotic systems have structure complexity, therefore the encryption algorithm involved the generated random sequence based on chaotic maps can have high complexity, which is good for cryptosystem. In addition, the control parameters of the chaotic system are in fact the secret key of the cryptosystem. To increase the number of control parameters can increase the size of the key space, making the algorithm archive higher security level. To sum up, to use multiple chaotic maps is potential way to increase the robustness of the encryption algorithm.

In this paper, we propose a novel encryption approach to enhance the security level of cryptosystem by introducing bit planes decomposition, together with the use of multiple chaotic maps as key generators to shuffle each bit plane. The cryptosystem has two stages; confusion stage and diffusion stage. In confusion stage, instead of permuting each pixel of the image (8 bits), which does not change the color histogram of the image [9], [10], partitioning the input image into eight bit planes first and recomposing eight bit planes afterward can totally change all pixel values. Therefore, the color histogram of the image at this stage differs from that of the original one. Also, when permuting each bit plane, eight bit planes are shuffled independently using eight key generators based on different chaotic maps with all different initial parameters/control parameters. After the confusion process, XOR operation is taken with a random bit matrix generated from another chaotic map in order to

Manuscript received May 25, 2014; revised August 20, 2014.

doi: 10.12720/ijsps.3.1.8-13

hide the characteristics of the original image completely. The combination of bit planes decomposition and the chaotic maps enhances the complexity of the encryption algorithm, making it more resistance to different attacks.

The remainder of this paper is organized as follows. Section 2 presents the selection of the chaotic maps for each stage of the proposed encryption scheme. Section 3 describes the proposed image encryption method. Section 4 shows the experimental results and the security analysis. Finally Section 5 concludes the paper.

II. Chaotic Maps

In chaos-based encryption techniques, the chaotic systems are typically used for generating pseudo random sequences to permute pixels of the input image in the confusion stage. Typically the input image pixels will be randomly shuffled based on the chaotic map in this stage; however, the value of each pixel still does not change. In this paper, we design a new encryption scheme, which will decompose the image into eight bit planes first, and then shuffle each bit plane separately based on different chaotic maps. So, when we recompose bit planes into an image, all pixel values change completely at this stage, hiding the characteristics of the plain image. In this design, we need to use multiple chaotic maps. Three types of chaotic maps are chosen as choices of key generators for different bit planes. The discretized standard chaotic map and logistic map are selected because of their simplicity to implement due to their simple mathematical formulas. And, Tinkerbell chaotic map is chosen, since it has multiple control parameters, and the map offers different chaotic behaviors, giving higher complexity to overall encryption algorithm.

A. Standard Chaotic Map

The mathematical model of the standard chaotic map is

$$\begin{aligned} a_{i+1} &= (a_i + b_i) \bmod 2\pi, \\ b_{i+1} &= (b_i + k\sin(a_i + b_i)) \bmod 2\pi, \end{aligned} \tag{1}$$

where k, k>0 is the control parameter, and (a_i, b_i) is the i^{th} state taking real values in [0, 2π) for all i.

B. Discretized Standard Map

The formulation of the discretized standard map is

$$\begin{aligned} x_{i+1} &= (x_i + y_i) \bmod N \\ y_{i+1} &= (y_i + K\sin(\frac{2\pi x_{i+1}}{N})) \bmod N \end{aligned} \tag{2}$$

where N is the width or length of image, and K is secret key which serves as a control parameter.

C. Logistic Chaotic Map

The mathematical model of logistic map is

$$x_{i+1} = rx_i\,(1 - x_i) \tag{3}$$

where x_0 is primary value and r is control parameter which has value between 3.57 and 4

D. Tinkerbell Chaotic Map

Tinkerbell chaotic map [11] has the formulation of the system as follows.

$$\begin{aligned} x_{i+1} &= x_i^2 - y_i^2 + ax_i + by_i \\ y_{i+1} &= 2x_i y_i + cx_i + dy_i \end{aligned} \tag{4}$$

where x_0 and y_0 are initial values and a, b, c, and d are control parameters. This offers larger key space, since there are multiple control parameters. The behaviors of Tinkerbell chaotic system is shown in Fig. 2.

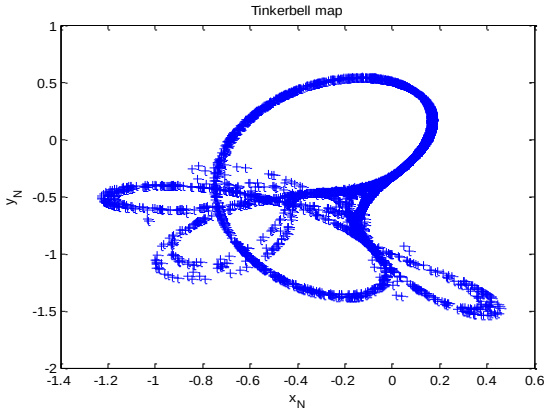


Figure 2. Tinkerbell map with a=0.9, b=−0.6013, c=2, d=0.5, and initial values of x_0=−0.72, y_0=−0.64

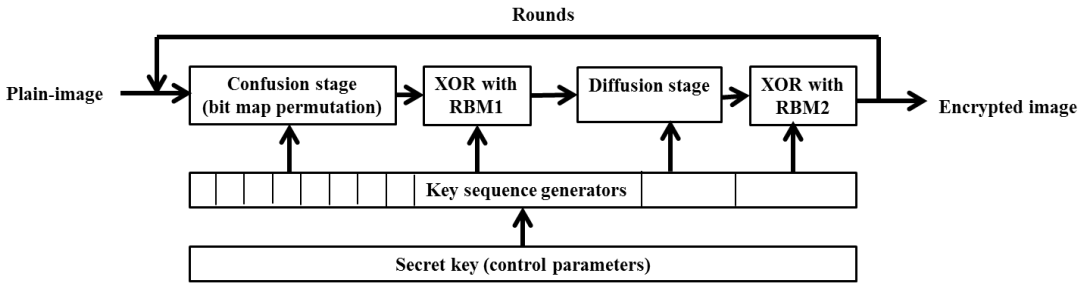


Figure 3. The architecture of the proposed image encryption method

III. Proposed Encryption Method

The proposed encryption method (Fig. 3) has two major stages; confusion and diffusion stage. The main techniques of the proposed scheme are to decompose the image into eight bit planes, and to use multiple chaotic maps as key sequence generators. In the confusion stage (Fig. 4), permutations are applied independently for each bit plane, followed by XOR operation with random bit matrix generated by the chaotic map based on the same

secret key, then recomposing the image and outputting the image to the diffusion stage.

A. The Confusion Stage

The confusion stage of the proposed method is shown in Fig. 4.

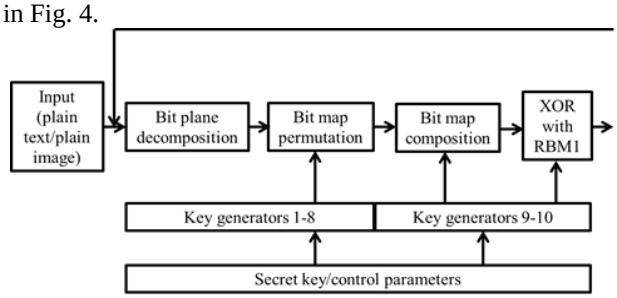


Figure 4. The confusion stage of the proposed cryptosystem

The first step of the confusion stage is to apply bit plane decomposition (Fig. 5).

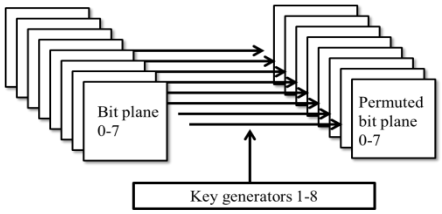


Figure 5. Bit plane decomposition

Step 1: Decompose the input image into eight bit planes

Step 2: For each bit plane, use corresponding key generator to perform the permutation

1. Get initial conditions from the secret key
2. Choose the key generator base on the plain image and the secret key
3. Let F be the chaotic functions
4. Iterate $x_{n+1} = F(x_n)$ for $M \times N$ times and get a sequence $X = \{x_1, x_2, x_3, ..., x_{M \times N}\}$
5. Sort the sequence X in the descending order to obtain a new sequence $X' = \{x_1', x_2', x_3', ..., x_{M \times N}'\}$
6. Find the positions of X' in X and store the positions in $Index_t = \{ind_1, ind_2, ind_3, ..., ind_{M \times N}\}$, $t = 1, 2, 3, ..., 8$
7. Shuffle $Bitplane\ 0-7$ based on $Index_t$

Step 3: Recompose the eight bit planes into one image

Step 4: Perform XOR operation with a random bit matrix (RBM1) generated from the selected chaotic map.

B. The Diffusion Stage

The diffusion stage of the proposed method is shown in Fig. 6.

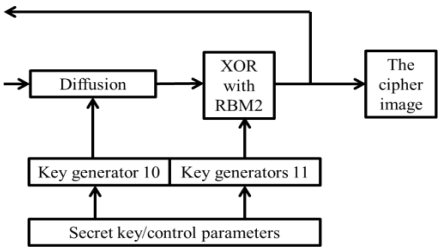


Figure 6. The diffusion stage of the proposed cryptosystem

Let I be the source image of the size $M \times N$

Step 1: Generate the sequence J from the image I, $J(0)$ is the first element of the image

Step 2: Shuffle the sequence J to get a new sequence J' based on $Index_9$

Step 3: Diffuse the image with this function

$$J'(k) = J'(k-1) \oplus J'(k), k = 1, 2, 3, ..., M \times N$$

Step 4: Iterate the step 2-3 until satisfying the requirement

Step 5: *Bitxor* with the random bit matrix (RBM2) generated from another chaos-based key generator

Step 6: Done when finishing the iteration rounds

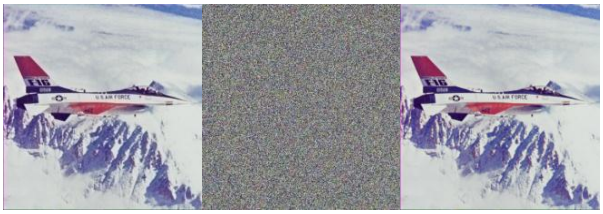
Note that the decryption method is similar to that of encryption but do all operations in the reverse order manner.

IV. Experimental Results and Security Analysis

In the experiment, we implement the image encryption method on MATLAB software. We use different test images such as Lena 512×512, Baboon 512×512, and Airplane 512×512, and also experiment with different sizes of image such as Lena 128×128, Lena 256×256, and Lena 512×512. The experimental results are shown in Fig. 7. We evaluate the performance and the security by using the statistical analysis, key space analysis, and key sensitivity analysis.

(a) Lena 512×512 (b) encrypted image (c) decrypted image

(a) Baboon512×512 (b) encrypted image (c) decrypted image



(a) Airplane512×512 (b) encrypted image (c) decrypted image

Figure 7. (a) The original images (b) the corresponding encrypted images, (c) the corresponding decrypted images

A. Statistical Analysis

- Histogram

Histogram shows how the intensity values of image pixels are distributed. A good encryption should be able to hide the characteristics of the original image. So, the ideal histogram of the encrypted image is uniform. Fig. 8, Fig. 9, and Fig. 10 show the histograms in all color channels of the plain-images and encrypted images of Lena, Baboon, and Airplane image respectively. The result shows that the histograms in all color channels of the encrypted images are very close to uniform distribution, and the histograms of the encrypted images are totally different from the histograms of the original images, so they do not provide any clue for statistical attackers and differential attackers on the encrypted image. This means that this encryption scheme is very robust and secure.

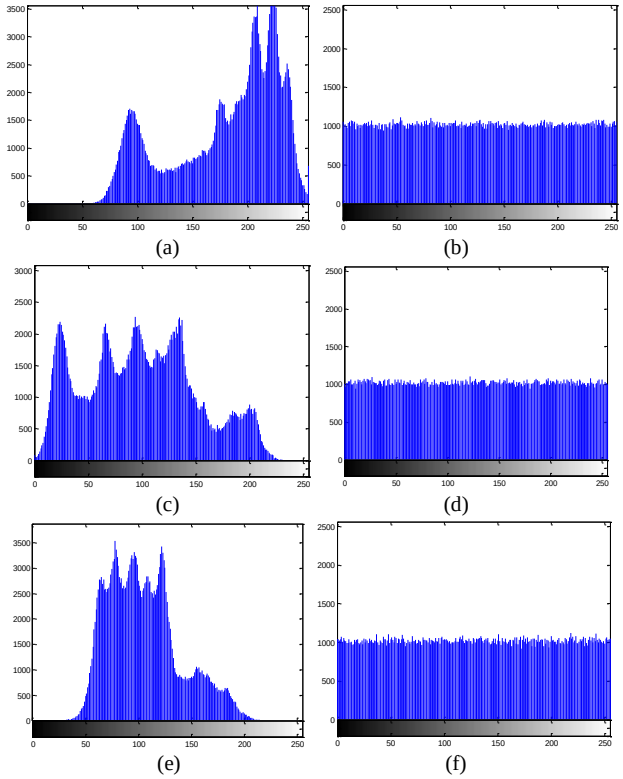
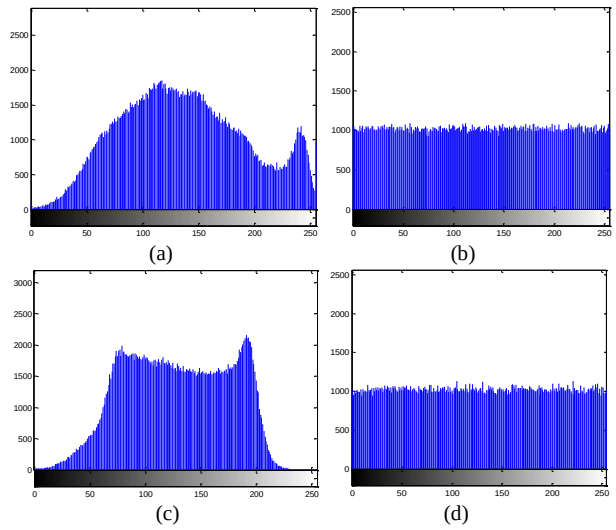


Figure 8. (a) (c) (e) Histogram of the plain-image "lena 512×512" in red, blue, green channel respectively, (b) (d) (f) Histogram of encrypted image in red, blue, green channel respectively



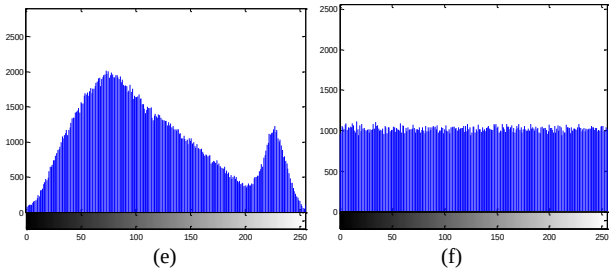


Figure 9. (a) (c) (e) Histogram of the plain-image "baboon 512×512" in red, blue, green channel respectively, (b) (d) (f) Histogram of encrypted image in red, blue, green channel respectively

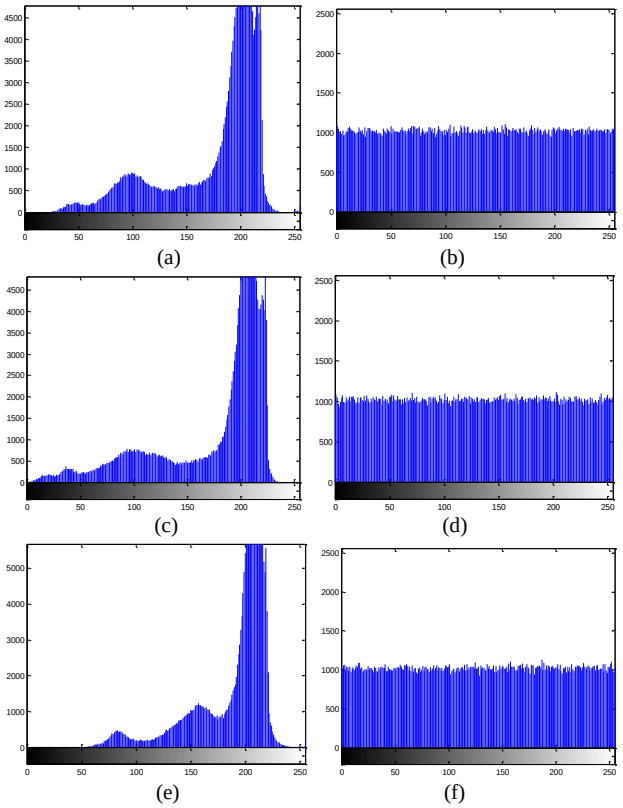


Figure 10. (a) (c) (e) Histogram of the plain-image "airplane 512×512" in red, blue, green channel respectively, (b) (d) (f) Histogram of encrypted image in red, blue, green channel respectively

- Information entropy

The entropy in color image is the value that evaluates the probability distribution of each intensity levels image. The entropy of the image can be computed using (5).

$$H(x) = -\sum_{i=1}^{N} p(x_i)\log_2 p(x_i) \quad (5)$$

where $p(x_i)$ is the probability of intensity level x_i

If each intensity level appears with equal probability $1/N$, the maximum entropy is $\log_2 N$. Entropy in each channel of the color image has max value of $\log_2 256 = 8$. In a good encryption, the entropy value of encrypted image should be higher than the entropy value of the plain-image. The results in Table I show that the entropy of encrypted image is superior to that of [12]-[15]. Moreover, the entropy values of the encrypted image are very close to the theoretical value of max entropy. This

means that the proposed encryption method has security superiority, and resists against entropy attack.

TABLE I. INFORMATION ENTROPY OF PLAIN-IMAGE AND ENCRYPTED IMAGE

Plain image	Entropy of	
	Original image	Encrypted image
Lena	7.750197	7.999770
Baboon	7.762436	7.999761
Airplane	6.663908	7.999757

- Correlation of adjacent pixels in all directions

Assume that we test N pairs of adjacent pixels

Let x be the intensity value of the pixel (i, j)

Let y be the intensity value of the pixel $(i+1, j)$, $(i, j+1)$ or the pixel $(i+1, j+1)$

The correlation coefficients can be computed using (6).

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2)(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2)}}, \quad (6)$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

For strong encryption, the correlation coefficients should have the value close to zero. The results in Table II demonstrate the effectiveness of the method, since the correlation coefficients in all directions and all color channels are very close to zero. The correlation coefficients of encrypted images are superior to the scheme [12]-[15].

TABLE II. THE CORRELATION COEFFICIENTS IN ALL DIRECTIONS AND ALL COLOR CHANNELS OF THE TEST IMAGE AND ENCRYPTED IMAGE

image	channel	direction		
		horizontal	vertical	diagonal
Original image (Lena)	R	0.9798	0.9893	0.9697
	G	0.9691	0.9825	0.9555
	B	0.9327	0.9576	0.9183
Encrypted Image (Lena)	R	0.0024	-0.0001	0.0022
	G	-0.0013	0.0032	-0.0004
	B	0.0002	-0.0036	0.0011
Original image (Baboon)	R	0.9231	0.8660	0.8543
	G	0.8655	0.7650	0.7348
	B	0.9073	0.8809	0.8399
Encrypted Image (Baboon)	R	-0.0018	0.0001	-0.0004
	G	0.0016	0.0025	0.0030
	B	-0.0017	-0.0015	-0.0034
Original image (Airplane)	R	0.9726	0.9568	0.9343
	G	0.9578	0.9678	0.9326
	B	0.9640	0.9353	0.9146
Encrypted Image (Airplane)	R	0.0016	0.0003	-0.0004
	G	0.0005	-0.0013	-0.0045
	B	0.0005	-0.0018	-0.0004

The image correlation tests, including horizontal, vertical, and diagonal direction between adjacent pixels of plain image and encrypted image are shown in Fig. 11. The results show that there are strong correlations among adjacent pixels in the plain-image, and the correlations are significantly reduced in the encrypted image.

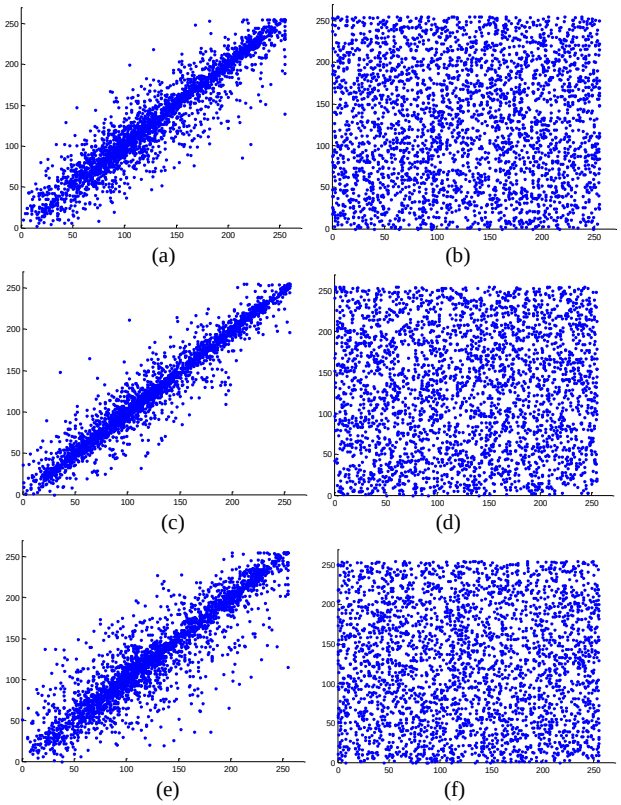


Figure 11. Image correlation tests in original image and encrypted image, including (a) (b) horizontally, (c) (d) vertically, (e) (f) diagonally adjacent pixels

B. *Key Space Analysis*

Key space size is the total number of different keys, which can be used as the control parameters in the encryption method. A good encryption method should have a large enough key space to resist brute-force attack. From the method proposed in Section 3, the use of multiple chaotic systems requires initial conditions for all systems. For eleven key generators, we use double floating point as our key. Since each generator has at least one floating point as the initial parameters. The proposed system has a minimum key size of $11 \times 64 = 704$ bits in total. Thus, the key space of the proposed algorithm is at least 2^{704}. According to IEEE floating point standard, the key space of our scheme finely passes the minimum requirement of DES, which is 2^{128}.

C. *Sensitivity Analysis*

In order to resist brute force attack and differential attack, a good encryption method should be sensitive to the key and the plain-image. This means that if the key or the plain-image has tiny change, the encrypted image should be totally different.

The common measures are NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing

Intensity), which test the different rate between two images.

Let $c_1(i,j)$ and $c_2(i,j)$ denote the two images

$D(i,j)$ is 1 if $c_1(i,j)$ and $c_2(i,j)$ are different, else 0

NPCR and UACI can be computed as follows.

$$NPCR = \sum_{i,j} \frac{D(i,j)}{W \times H} \times 100\% \quad (8)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{c_1(i,j) - c_2(i,j)}{255}\right] \times 100\% \quad (9)$$

- Key Sensitivity

We encrypt the plain-image "lena 512×512" and encrypt with slightly different key which one bit different, resulting more than 99% of pixels between two encrypted images differ in gray value. Therefore, the proposed method provides strong key sensitivity.

- Plain image sensitivity

The sensitivity to the plain image implies how good the diffusion property of the encryption method is. We test this by changing one random pixel of the plain image, and see how much the encrypted image will change. Theoretically, the average different values between two uniformly distributed numbers between [0, 1] should be equal to 1/3 or 33.33%. Table III shows the measures of NPCR and UACI of the proposed encryption method.

TABLE III. NPCR AND UACI OF THE PROPOSED ENCRYPTION METHOD

Plain image	NPCR(%)	UACI(%)
Lena	99.25	33.82
Baboon	99.64	33.79
Airplane	99.88	33.57
average	99.59	33.73

The proposed encryption scheme obtains NPCR of 99.59% on average. This means that the method has high sensitivity to initial conditions/keys. And, the scheme obtains UACI of 33.73% on average. This means that the proposed encryption method also has high sensitivity to the plain image, which is a property of good cryptographic system.

V. CONCLUSION

A highly secure and robust encryption method is obtained by using bit plane decomposition and multiple chaotic maps. The experimental results and the security analysis demonstrate that the proposed scheme is a very good encryption. It has good confusion and diffusion properties, large enough key space, strong secret key sensitivity, strong plain-image sensitivity, and uniformly distributed encrypted pixels, making it resistant to different attacks. Therefore, the security objective was archived. In the future work, the time computation issue of the algorithm should be considered, since our approach uses several key sequence generators and multiple permutations. So, taking the parallel computing at permutations of each bit plane might be alternative way to speed up the process.

REFERENCES

[1] K. Wang, W. Pei, *et al.*, "On the security of 3D cat map based on symmetric image encryption scheme," *Physics Letters A*, vol. 343, pp. 432-439, Aug. 2005.

[2] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, pp. 926-934, Sep. 2006.

[3] F. Y. Sun, S. T. Liu, Z. Q. Li, and Z. W. Lu, "A novel image encryption scheme based on spatial chaos map," *Chaos Solitions and Fractals*, vol. 38, no. 3, pp. 631-640, Nov. 2008.

[4] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optic Communications*, vol. 282, pp. 2123-2127, Jun. 2009.

[5] C. Fu, W. H. Meng, *et al.*, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp. 1000-1010, Sep. 2013.

[6] A. Mousa, E. M. El-Rabaie, *et al.*, "Images cryptosystem based on chaotic maps for databases security," presented at the IEEE 2nd International Japan-Egypt Conference on Electronics, Communications, and Computers, Dec. 17-19, 2013.

[7] X. Li, "Image encryption scheme based on multiple chaotic maps," presented at the IEEE International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), Xi'an, China, Sep. 9-11, 2013.

[8] F. Chong, H. Shuai, *et al.*, "A chaos-based image encryption scheme with a plaintext related diffusion," presented at the IEEE Int. Conf. on Information, Communications and Signal Processing, Taiwan, Dec. 10-13, 2013.

[9] G. J. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, pp. 2775-2780, Jun. 2011.

[10] H. T. Panduranga, S. K. Naveenkumar, *et al.*, "Partial image encryption using blockwise shuffling and chaotic map," presented at International Conference on Optical Imaging Sensor and Security, India, Jul. 9-12, 2013.

[11] A. Goldsztejn, W. Hayes, and P. Collins, "Tinkerbell is chaotic," *SIAM J. Applied Dynamical Systems*, vol. 10, pp. 1480-1501, Dec. 2011.

[12] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, pp. 347-354, Apr. 2010.

[13] Z. L. Zhu, W. Zhang, *et al.*, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, pp. 1171-1186, Mar. 2011.

[14] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, pp. 3895-3903, Aug. 2011.

[15] C. Fu, B. Lin, Y. Miao, X. Liu, and J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, pp. 5415-5423, Nov. 2011.

Wipawadee Auyporn was born in Nakhon Ratchasima province, Thailand, in 1988. She received the B.Sc. degree from Brown University, in 2011 in Computer Engineering with specialty in Multimedia Signal Processing. She is currently pursuing a M.Eng. degree in Computer Engineering at Chulalongkorn University. Her research interests include digital image processing for security, cryptography, and information theory.

Sartid Vongpradhip is the associate professor in the department of computer engineering, Chulalongkorn University since 1982. He earned B.Sc. (Honors) in electrical engineering from Newcastle upon Type Polytechnic, in 1979, and M.Sc. in electronic and electrical engineering from King's College University of London in 1981, and Ph.D. in computer engineering from University of Technology Sydney, in 1994. He has research interests including digital systems, digital circuits testing, fault tolerant computing, digital watermarking, QR code, and data hiding in image, etc.