Security Analysis of Selective Image Encryption Algorithm Based on Chaos and CBC-like Mode

Rinaldi Munir
School of Electrical Engineering and Informatics (SEEI)
Bandung Institute of Technology, ITB
Bandung, Indonesia
rinaldi-m@stei.itb.ac.id

Abstract—**This paper present a security analysis of the proposed selective image encryption algorithm based on chaos and CBC-like mode. The algorithm uses a Logistic Map to generate kesytreams that XOR-ed with 4-bit MSB of each pixel. Security analysis covers key space analysis, histogram analysis, correlation analysis, entropy analysis, and sensitivity analysis. Based on experiment results and the security analysis can be concluded that the proposed algorithm is secure from various attacks which aim to find the secret keys or pixels in plain-images.**

Keywords: selective, image, encryption, chaos, security analysys

I. INTRODUCTION

Nowadays, image is one of important message form, because images can present information visually and richer than text. Images play an important role in the multimedia industry today. Images are also video element, because a video is basically composed by a series of images.

Currently digital images are not only stored in hard disks, flash disks, CDs, DVDs, and other memory devices, but also transmitted through public channels such as internet. Storage and transmission of images through transmission channels are vulnerable to access or interception by unauthorized parties. Therefore, it is important to protect the confidentiality of images from unauthorized access. Image encryption has been used extensively as a technique to maintain information security.

An image generally has a large data capacity, therefore any conventional encryption algorithms such as DES, AES, Blowfish, Serpent, RC4, RSA, ElGamal, Rabin, etc, are no longer suitable for image encryption. Some real-time applications such as teleconference, video live streaming, etc., obviously requires a very high computing speed that definitely does not fit the conventional algorithms to encrypt the images. Therefore, the solution to this problem is using concept of selective encryption as opposed to total encryption [2]. With this technique only a part of image components that need to be encrypted, but the effect is that overall image is encrypted. The purpose of selective encryption is to minimize computational volume during encryption and decryption process.

A special digital image encryption algorithm has been proposed [1]. The algorithm is based on combining chaos and selective approach. Chaos-based encryption becomes an attractive research topic today [3]. Chaos system is used in cryptography for three reasons: (1) the nature of chaos is sensitive to initial conditions of the system, (2) random chaotic behavior, and (3) the values do not have a period of chaos.

To obtain the cipher-image are resistant to frequency analysis, we used modes such as CBC (cipher block chaining) so called CBC-like [4]. With this mode the same plain-pixels does not produce the same cipher-pixels. If it is applied to the image, pixels in the plain-image and pixels in the cipher-image has no statistical relationship so that the cryptanalyst is difficult to deduce the key or plain-image

In this paper we present security analysis of selective image encryption algorithm that proposed in [1]. Security analysis cover key space analysis, histogram analysis, correlation analysis, entropy analysis, and sensitivity analysis.

II. PROPOSED ALGORITHM

The proposed selective image algorithm [1] encrypts images in spatial domain. Only 4-bits of MSB of every pixel that need to be encrypted based on results in [5], so that computation volume is reduced to 50%. To obtain the cipher-image has no statistical relationship with its plain-image, then a CBC-like mode is used for encryption as shown in Fig. 1. P_i (i = 1,2, .. n) is 4-bit of MSB of pixel, C_i (i = 1,2, .. n) is 4-bits of MSB of encrypted pixel, and K_i (i = 1,2, .. n) is 4-bits keystream. Encryption with CBC-like mode can be expressed as follows:

$$C_i = E_{K_i}(P_i \oplus C_{i-1}) \quad (1)$$

and decryption is expressed as

$$P_i = E_{K_i}(C_i) \oplus C_{i-1} \quad (2)$$

Function E in Fig. 1 is

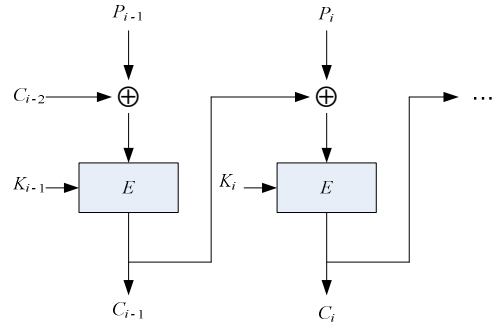
$$E_{K_i}(X_i) = X_i \oplus K_i \quad (3)$$

where $X_i = P_i \oplus C_{i-1}$ in encryption scheme and $X_i = C_i$ in

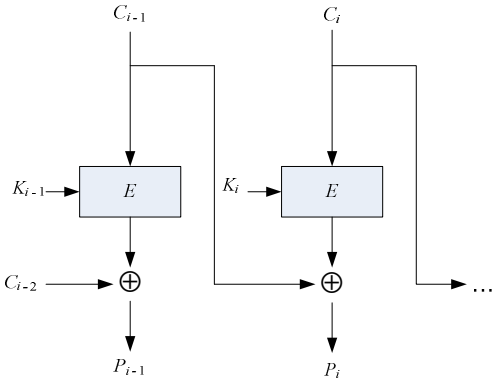
decryption scheme. K_i is generated form a logistic map,

$$x_{i+1} = r\, x_i\, (1 - x_i) \qquad (4)$$

where $0 \le x_i \le 1$, $i = 0, 1, 2, \ldots$ and $0 \le r \le 4$. Initial value of logistic map, x_0, and constant r serve as secret keys. Four-bit keystream K_i obtained as follows: x_i multiplied by 10 repeatedly until it reach a desired long number (size), and then truncate to take the integer part. Last four bits of binary representation of the integer serve as K_i.



(a) Encryption



(b) Decryption

Figure 1. Encryption and decryption scheme using CBC-like mode [1]

The proposed algorithm can be generalized to encrypt color images in which each for red channel (R), green (G), and blue (B) is encrypted separatedly.

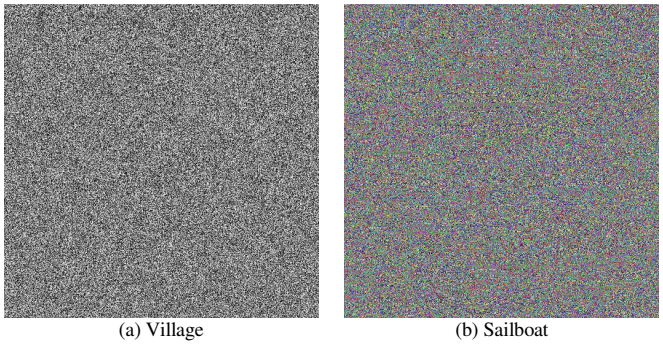
III. Experiment Results

Any grayscale or color images can be encrypted and then decrypted by the proposed algorithm above. Experiments are carried out using Matlab tool. Two images tested are 'village' (grayscale image) and 'sailboat' (color image) as shown Fig. 2(a) and 2(b). The key parameters are $x_0 = 0.45$ and $r = 3.999$. These parameters must be kept secret. The same keys is used to decrypt the cipher-images.

(a) Village (b) Sailboat

Figure 2. Two test images

Those test images are encrypted well by the algorithm and the key parameters. The results are shown in Figure 3. The encrypted images look like random images and can not be recognized anymore. The encrypted images can be decrypted back into the original images exactly.



(a) Village (b) Sailboat

Figure 2. The encrypted images

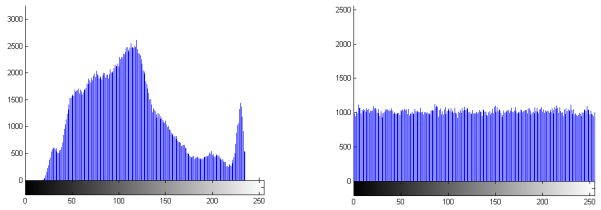
IV. Security Analysis

In this section we discuss security analysis of the experimental results above. As mentioned in Section I, security analysis covers histogram analysis, correlation analysis, entropy analysis, sensitivity analysis, and key space analysis.

A. *Histogram Analysis*

Histogram shows distribution of pixel intensities of an image. Using histogram an attacker does frequency analysis to deduce the secret key or plain-pixels. This kind of attack is called statistical attack. To prevent statistical attack, histogram of plain-image and histogram of cipher-image should not have a similarity statistically. Therefore, histogram of cipher-image should be relatively flat or statistically have an uniform distribution. Relatively uniform distribution of the cipher-image is an indication that the image encryption algorithm has a good quality [6].

Figure 3 (a) and (b) show histograms of image 'village' before and after encryption. Histogram of cipher-image looks flat and significantly different from histogram of plain-image.

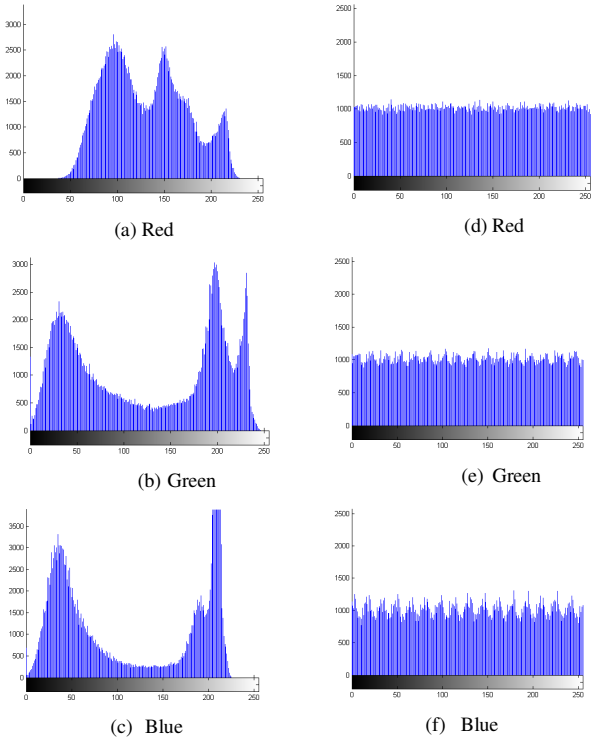


(a) Before encryption (b) After encryption

Figure 3. (a) Histogram of plain-image 'village'; (b) histogram of cipher-image 'village'

Figure 4 (a) through (c) show the histogram of plain-image 'sailboat' for each RGB color channel while Figure 4 (d) to 4 (f) show histogram of each color channel of cipher-image. Just as image 'village' histogram of each color looks flat too.

Based on the experiment results above, flat histogram in cipher-images can make an attacker difficult to deduce pixel values or secret keys using statistical attack.



(a) Red (d) Red

(b) Green (e) Green

(c) Blue (f) Blue

Figure 4. (a)-(c) Histogram of image 'village' (*plain-image*) for each color *RGB*; and (d)-(f) histogram of cipher-image for each color.

B. Correlation Analysis

Statistical correlation is a measure that states strength of linear relationship between two random variables. Let x and y are two random variables, each consisting of n elements, correlation coefficient of the two random variables is calculated by equation:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{5}$$

where

$$\mathrm{cov}(x, y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \tag{6}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \tag{7}$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i \tag{8}$$

To determine the correlation of pixels in the encrypted image, we calculate the correlation coefficient between two horizontally neighboring pixels [$f(i, j)$ and $f(i, j + 1)$], two vertically neighboring pixels [$f(i, j)$ and $f(i +1, j)$], and two diagonally neighboring pixel [$f(i, j)$ and $f(i +1, j +1)$]. Randomly we select 1000 pairs of neighboring pixels in each direction (vertical, horizontal, and diagonal), each for plain-image and cipher-image. Without loss of generalization, correlation analysis performed on grayscale images only. The correlation coefficients for image 'village' is calculated by equation (5), which in this case x and y are grey values of two neighboring pixels. The results of correlation calculations are shown in Table 1.

Table 1. Comparison of correlation coefficient between two neighboring pixels

Correlation coefficient	Horizontal	Vertical	Diagonal
Plain-image	0.9703	0.9599	0.9435
Cipher-image	-0.0038	-0.0401	-0.0219

In any natural-image, neighboring pixels have a strong linear relationship. It is characterized by a high correlation coefficient (close to +1 or -1). Table 1 shows that it is true that the correlation coefficient in the plain-image is close to 1. By contrast, in random image, the coefficient correlation between neighboring pixels are close to zero. Table 1 again shows that the correlation coefficient in the cipher-image is close to 0. So, the proposed image encryption algorithm successfully make correlation of neighboring pixels in the cipher-image becomes weak or close to zero.

To see more clearly, Figure 5 shows distribution of neighboring pixels. Left column is distribution of the plain-image correlation and right column is distribution of the cipher-image correlation. In plain-image we can see that the neighboring pixels values were around 45° diagonal line, which indicates a strong correlation between the pixels. In contrast, values of cipher-image pixel values are spread evenly throughout the plane, which indicates the pixels in it are no longer correlated.

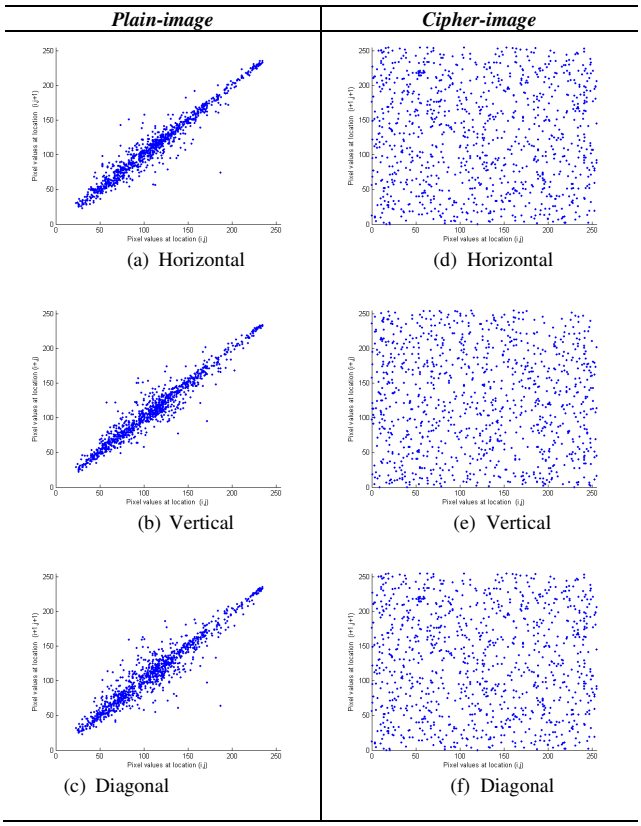


Figure 5. Distribution of correlation of neighboring pixels in the plain-image and the cipher-image of 'village'

C. Entropy Analysis

Refer to information theory, entropy states degree of uncertainty in a system. Entropy of message m is calculated by equation [6]:

$$H(m) = \sum_{i=0}^{2M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (9)$$

$P(m_i)$ in Eq. (9) states probability simbol m_i in a message. Entropy is expressed in units of bits. Random messages should have an ideal entropy equal to 8, while in less random message its entropy is less than eight. If the entropy is less than eight, there are degrees of predictability, which is a threat to security [6].

Cipher-images can be viewed as random images, so the entropy should ideally 8. In the grayscale image there are 256 gray values ($m_0 = 0$, $m_1 = 1$, ..., $m_{255} = 255$) and probability of each grey value is calculated from its histogram. Without loss of generalization, we calculate an entropy for grayscale image only. For cipher-image in Figure 2(a) the entropy is

$$H(m) = \sum_{i=0}^{255} P(m_i) \log_2 \frac{1}{P(m_i)} = 7.9991$$

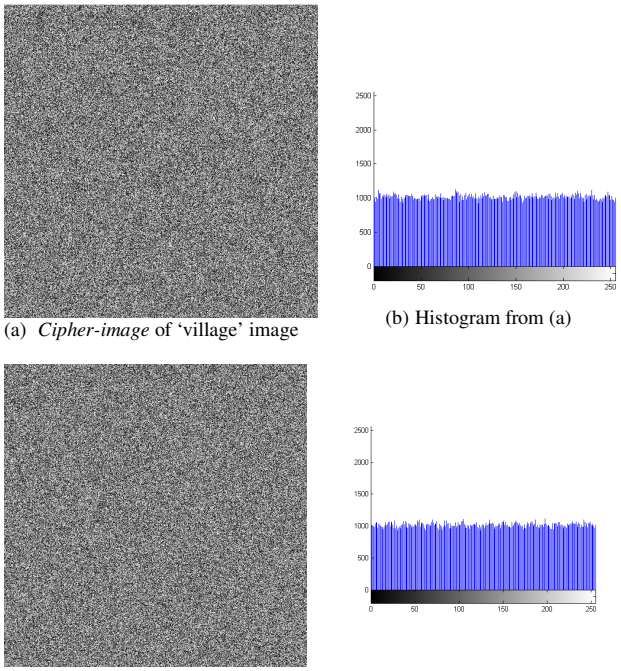
This entropy (7.9991) is very close to 8 which means that the proposed selective encryption algorithm is safe from entropy attack that predict information in the image.

D. Sensitivity Analysis

One of characteristics of chaos is the sensitivite to small changes in initial values. When applied to image encryption means if encryption key is changed slightly then decryption process produces another cipher-image significantly different (failed to return the cipher-image into the original plain-image).

Refer again to proposed algorithm in Section II. In the algorithm, Logistic Map is used to generate chaos values, extract four bits from the value, and then XORed with the 4-bits of the pixel. Small change to initial value (x_0) make random values generated from the Logistic Map significantly different after Logistic Map iterated a number of times. As a result, the keystream also differ significantly, and XOR operation gives a significantly different image.

Let x_0 is changed so that it becomes $x_0 + \Delta$, then the cipher-image is decrypted with the key. Let $\Delta = 10^{-10}$ so that the initial value of a logistic map 0.4500000001. Figure 9 shows decryption result of the cipher-image 'village'. Output of the decryption has remained scrambled. This experiment shows that sensitivity characteristics of chaos provide good security from exhaustive attack. Small change of the secret key causes decryption process produces wrong image.



(a) *Cipher-image* of 'village' image

(b) Histogram from (a)

(c) 'village' image after decryption (with small change to x_0)

(d) Histogram from (c)

Figure 6. Sensitivity experiment with small change to x_0 of $\Delta = 10^{-10}$.

E. Key Space Analysis

Space key states of different number of keys that can be used to do the encryption / decryption [7]. In order to make brute-force attack not effective, then the key space should be made large enough. The secret keys used in the proposed encryption algorithm is x_0 and r, both are real numbers. According to standard 64-bit IEEE floating-point, computation precision of the floating point is 10^{-15} [7], so number of possible values of x_0 is 10^{15} as well as r. Thus, key space is $10^{15} \times 10^{15} = 10^{30}$. This key space is large enough so that the algorithm can be resistant to brute-force attack.

V. CONCLUSIONS

Security analysis of a proposed selective image encryption algorithm based on chaos has been presented. Security analysis covers histogram analysis, correlation analysis, entropy analysis, sensitivity analysis, and key space analysis. Histogram analysis shows that histogram of cipher-image is flat or uniformly distributed, so the algorithm is secure from frequency analysis attack. Correlation analysis shows that pixels in cipher-image does not correlate one another, so the algorithm is secure from statistical analysis attack to find the key or plain-image. Entropy analysis show that the algorithm has entropy that close to ideal entropy (8), so the algorithm is secure from leakage of information. Sensitivity analysis shows that the change in initial values of chaos shows that the algorithm is secure from-exhaustive key search attack. Finally, key space analysis shows that the number of possible keys is very large so the algorithm is secure from a brute-force attack. Overall the proposed selective image encryption algorithm is secure from attack to find the key or pixels in the plain-image.

ACKNOWLEDGMENT

Research that published in this paper is fully supported by a grant for Riset dan Inovasi KK (ITB Research Program 2012).

REFERENCES

[1] Rinaldi Munir, "Pengembangan Algoritma Enkripsi Selektif Citra Digital dalam Ranah Spasial dengan Mode *CBC-like* Berbasiskan *Chaos*, Prosiding SITIA 2012, Institut Teknologi 10 November, Surabaya, 2012.

[2] Nidhi S Kulkarni, Balasubrmanian Raman, Indra Gupta, *Selevtive Encryption of Multimedia Image*s, Proc. Of XXXII National Systems Conference, NSC 2008, December 17-19, 2008.

[3] James Lampton, *Chaos Cryptography: Protecting data Using Chaos,* Missisippi School for Mathematics and Science.

[4] Bruce Schneier, *Applied Cryptography 2nd Edition*, Wiley & Sons, 1996.

[5] Tao Xiang, Kwok-wo Wong, Xiaofeng Liao, *Selective Image Encryption Using a Spatiotemporal Chaotic System*, Chaos Volume 17, 2007.

[6] Alireza Jolfaei, Abdul Rasoul Mirghadri, *An Image Encryption Approach Using Chaos and Stream Cipher*, Journal of Theoretical and Applied Information Technology, 2010.

[7] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, Y. Yu. 2012. A Chaos-based Digital Image Encryption Scheme with an improved Diffusion Strategy. *Journal Optic Express 2363*, *Vol. 20. No. 3*.