Robustness Analysis of Selective Image Encryption Algorithm Based on Arnold Cat Map Permutation

Rinaldi Munir
School of Electrical Engineeringline and Informatics
Institute Technology of Bandung, ITB
Bandung, West Java, Indonesia
rinaldi-m@stei.itb.ac.id

***Abstract*—Image encryption in frequency domain has an advantatge of resistance to many image processing operations. This paper presents a robustness analysis of a proposed selective image encryption algorithm based on chaos. The cipher-images was modified by common image processings such as JPEG compression, adding noise, brightness/contrast adjustment, and image resizing. Based on experiment results, the cipher-images were robust to the image processing operations, since the modifications have little influence on low frequency DCT coefficients. The decrypted images can be still recognized well, although they are just like noised.**

Keywords*: *image encryption, chaos, robustness analysis.

I. INTRODUCTION

In information technology era, images play important role in representing information. Images can be transmitted through public channel such as internet and also sored in the storage devices. Storage or transmission of images through transmission channels in the form of plain-images have has risks. The plain-images are vulnerable to access or interception by unauthorized parties. Therefore, the confidentiality of plain-images need to be protected from unauthorized acces. Solution to this problem is to encrypt them so that the images can not be recognized anymore. Image encryption has been used extensively as a technique to maintain information security.

Actually any conventional encryption algorithms such as DES, AES, Blowfish, Serpent, RC4, RSA, ElGamal, Rabin, etc, can be used to encrypt images, but the algorithms are no longer suitable for image encryption because of an image generally has a large data capacity. 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. To overcome the weakness of the conventional algorithms, concept of selective encryption --as opposed to total encryption-- then be used [2]. Selective encryption means that only a part of image components that need to be encrypted, but the effect is overall image is encrypted. Purpose of selective encryption is to minimize computational volume during encryption and decryption process.

The images can be encrypted in spatial domain, frequency domain, or both. Two basic operations on image encryption is permutation (or scrambling) and substitution. Permutation changes the position of the pixels in the image, while subsitution changes pixel values. Permutation and/or substitution can be applied in the domain(s). However, scrambling in spatial domain has drawback that it keeps statistical characteristics of images after permutation [2]. To overcome the drawback of spatial domain scrambling, scrambling in frequency domain is performed.

A special digital image encryption algorithm based on chaos in frequency domain has been proposed [3]. The image is transformed by Discrete Cosine Transform (DCT), and the selected DCT coefficients is scrambled with Arnold Cat Map. Arnold Cat Map is 2-D chaos map that transforms an element from a position to another position in the same area [4]. Because of enciphering operation is done on DCT domain, the encryption methode is lossy and the decrypted images are not exactly same as the original images. However, since on DCT domain, the encrypted images are robust to many image processing, such as JPEG compression, noising, etc.

In this paper we present robustness analysis of selective image encryption algorithm that proposed in [3]. We measure the robustness of the selective encryption algorithm for image processing attack. Such image processings are JPEG compression, noising, resizing, brightness/contrast adjustment, etc.

II. PROPOSED ALGORITHM

The proposed selective encryption algorithm is based on the fact that the HVS (Human Visual System) is very sensitive at lower frequencies than higher frequencies [2]. Important visual information such as frame objects, shapes, etc., present in low frequency sub-bands, while the detailed information are contained in high frequency sub-bands (see Figure 1).

By encrypting only the DCT coefficients of the low frequency sub-band, then the visual information in the image to be damaged so that the image can not be recognized anymore (after doing IDCT), which means that the image was encrypted [3].

Supported by IEEE Indonesia Section, IEEE APS/MTT Indonesia Joint Chapter, and IEEE Communication Society (Comsoc) Indonesia Chapter ISBN 978-602-8509-18-3

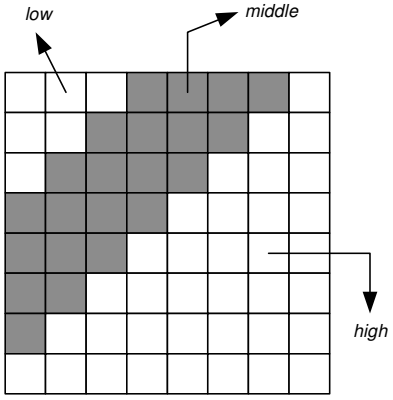


Fig 1. Three sub-bands of the *DCT* coefficients

Withous loss of generalization for color images, let I is an grayscale image of size $M \times N$ pixels. Outline of the proposed selective encryption algorithm is as follows [3]:

1. Perform image transform from the spatial domain into image to the frequency domain by DCT equation as follows:

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \quad (1)$$

where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}} & ,u = 0 \\ \sqrt{\frac{2}{M}} & ,1 \le u \le M-1 \end{cases} ; \quad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}} & ,v = 0 \\ \sqrt{\frac{2}{N}} & ,1 \le v \le N-1 \end{cases}$$

2. Scan DCT coefficients from matrix C with zig-zag algorithm, and then select the AC coefficients on low frequency sub-band as much as N^2 elements. DC coefficient is not selected because it carries important visual information in an image.
3. Place the selected AC coefficients into a matrix of size $N \times N$.
4. Apply Arnold Cat Map (with secret parameters b and c) to scramble the selected AC coefficients above m times. The Arnold Cat Map is

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N) \quad (2)$$

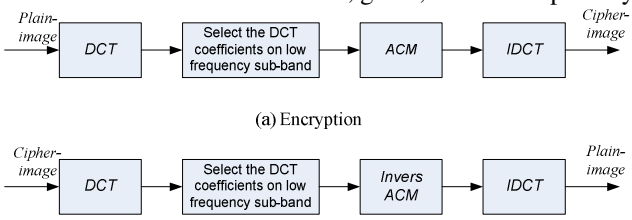
(Note: For the decryption process we use inverse of the Arnold Cat Map i.e:

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod(N) \quad (3)$$)

5. Put back the scrambled AC coefficients into matrix C.
6. Apply IDCT (inverse DCT) to matrix C to get the cipher-image. The IDCT equation is

$$I(x,y) = \alpha_u \alpha_v \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} C(u,v) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \quad (4)$$

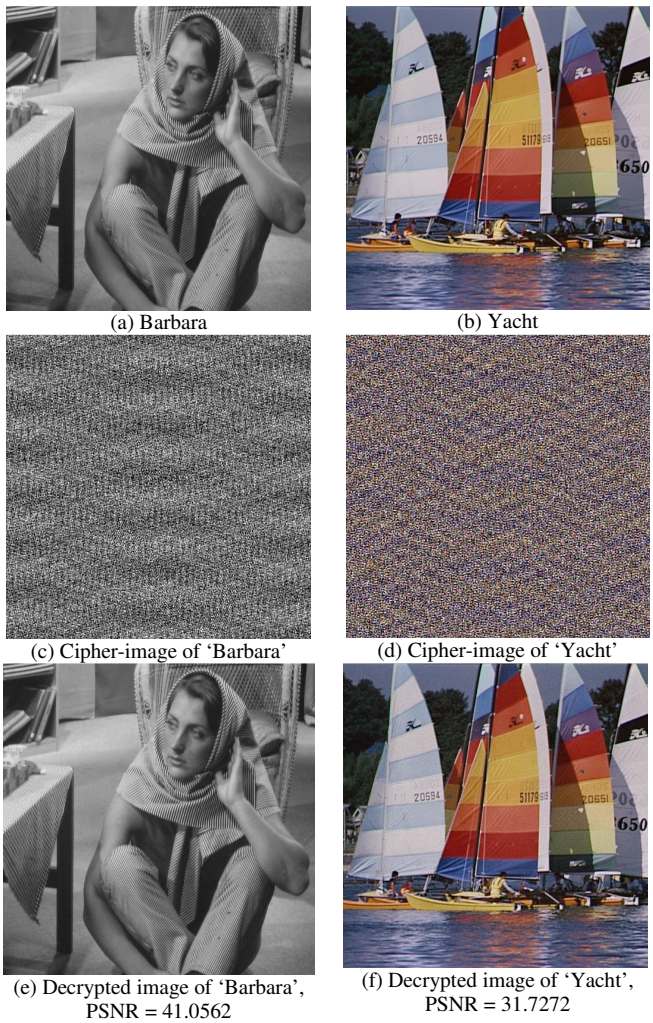
Figure 2 shows each of encryption and decryption diagram of the proposed algorithm. For color images we apply the scheme to the channels of each red, green, and blue seperately.



(a) Encryption

(a) Decryption

Fig 2. An encryption and decryption diagram of the proposed algorithm [3].



(a) Barbara (b) Yacht

(c) Cipher-image of 'Barbara' (d) Cipher-image of 'Yacht'

(e) Decrypted image of 'Barbara', PSNR = 41.0562 (f) Decrypted image of 'Yacht', PSNR = 31.7272

Fig 3. (a) and (b) are plain-images; (c) and (d) are cipher-images; (e) and (f) are decrypted images.

Supported by IEEE Indonesia Section, IEEE APS/MTT Indonesia Joint Chapter, and IEEE Communication Society (Comsoc) Indonesia Chapter ISBN 978-602-8509-18-3

The secret keys of the algorithm are *b*, *c*, *m*, and *N*. Image decryption requires the same keys. Because of the DCT is a lossy transformation, then the image decryption does not yield exactly same as the original image. The proposed algorithm can encrypt both grayscale images and color images. The image size must be square to ensure the implementation of Arnold Cat Map. If the size is not square then it needs additional pixels so that the image size is square.

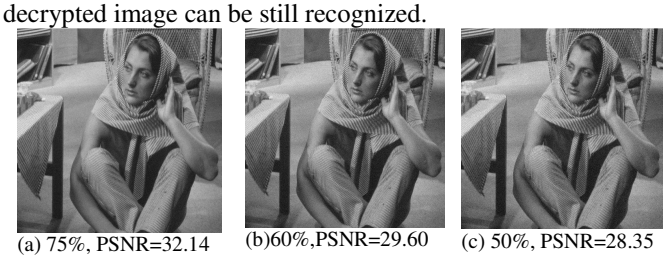
Fig. 3 shows two plain-images ('Barbara' image and 'Yacht' color image), the cipher-images, and the decrypted images. All images are 512 × 512 pixels. The secret keys are *b* = 47, *c* = 86, *N* = 300, and *m* = 5. A PSNR (peak-signal-to-noise-ratio) is calculated by formula $PSNR = 20 \times \log_{10}\left(\frac{b}{rms}\right)$, where *b* is peak signal (= 255 for grayscale image) and *rms* is an abbreviation of root mean square.

III. Experiments And The Robustness

Purpose of the experiments is to determine robustness of cipher-images to common image processings. Such image processings are JPEG compression, image noising, image resizing. etc. We use the *Photoshop* software to modify cipher-images. Without loss of generalization, the experiment is performed for grayscale image only ('Barbara' image).

3.1 JPEG Compression

We tested the robustness against JPEG compression with various compression qualities: 75%, 60%, 50%, 30%, 10%, and 5%. In this experiment we save the cipher-images of 'Barbara' of each compression quality into JPEG files using MATLAB code. Fig.4 shows the decrypted images of 'Barbara'. Quality of decrypted images (measured by PSNR) tends to decrease when quality of JPEG compression is reduced, but the decrypted image can be still recognized.



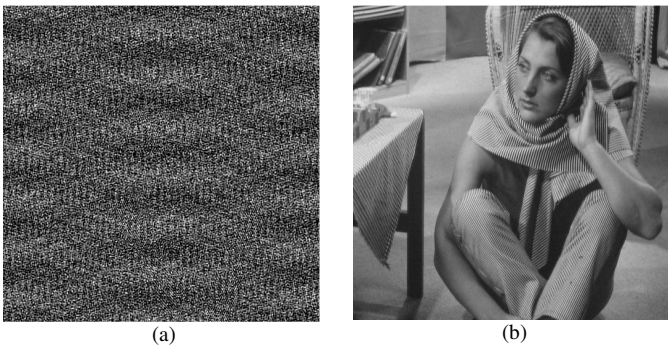
(a) 75%, PSNR=32.14 (b)60%,PSNR=29.60 (c) 50%, PSNR=28.35

(d) 30%, PSNR=25.41 (e)10%, PSNR=20.01 (f)5%, PSNR=17.36

Fig 4. The decrypted images of 'Barbara' when the corresponding cipher-images is compressed by JPEG with various compression quality.

3.2 Brightness/Contrast Adjustment

We use *Photoshop* software to adjust brigntness and contrast of cipher-image (the image brightness is reduced to factor -28 and contrast is increased to factor +30). Fig 5 shows the decrypted image after adjustment of the cipher-image. Since modification have little influence on low frequency DCT coefficients, the decrypted image also adjusted well.



(a) (b)

Fig 5. (a) Cipher-image after doing brightness/contrast adjustment; (b) The decrypted image (PSNR = . 41.0562)

3.3 Image Resizing

The cipher-image is resized by *Photoshop* software. In the first experiment we change the size of encrypted version of 'Barbara' image from 512 × 512 to 350 × 350 (reduction of), and in the second experiment we change from 512 × 512 to 1024 × 1024 (enlargement). After resizing, we resize it to original size before decryption. Fig. 6 shows the decrypted images after resizing. For reduction of the size, the decrypted image contains noise, but the image can still be recognized. For enlargment case, the decrypted image has a good quality.

(a) PSNR = 17.3145 (b) PSNR = 41.0562

Fig 6. (a) The decrypted image after reduction of the size; (b) The decrypted image after enlargment

3.4 Image Noising

In these experiments we add different noise to the cipher-image using Matlab code:

Supported by IEEE Indonesia Section, IEEE APS/MTT Indonesia Joint Chapter, and IEEE Communication Society (Comsoc) Indonesia Chapter ISBN 978-602-8509-18-3

```
J = imnoise(I,type)
```

Noise types are gaussian noise, poisson noise, salt and pepper noise, and speckle noise. For gaussian noise, a Matlab code is

```
J = imnoise(I,'gaussian',m,v)
```

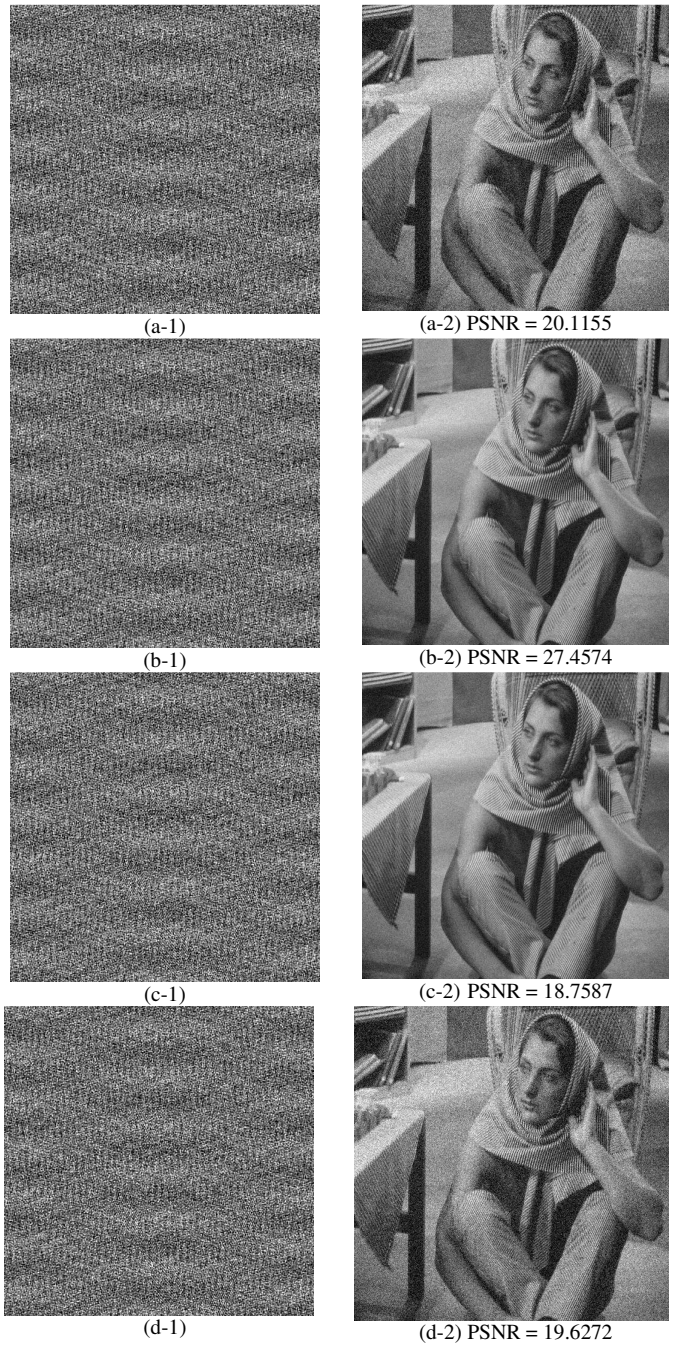


Fig 7. (a-1) Gaussian noise added; (b-1) Poisson noise added; (c-1) Salt & pepper noise added; (d-1) Speckle noise added. The second images in the right column are corresponding decrypted images.

The default values is zero mean (`m`) noise with 0.01 variance (`v`). For poisson noise, a Matlab code is

```
J = imnoise(I,'poisson')
```

and no default values. For salt and pepper noise, a Matlab code is

```
J = imnoise(I,'salt & pepper',d)
```

where `d` is the noise density. The default is 0.05 noise density. Finally, for speckle noise, a Matlab code is

```
J = imnoise(I,'speckle',v)
```

where `v` is the variance. The default for `v` is 0.04.

Fig. 7 shows the decrypted images after adding noise to the cipher-image. Overall the decrypted images contains noise, but the image can still be recognized.

IV. CONCLUSION

A robustness analysis of a proposed selective encryption algorithm based on chaos has been presented. The algorithm scrambles the selected low frequency DCT coefficients. To determine robustness of cipher-images to common image processings, some experments has been performed. Such image processings are JPEG compression, image noising, image resizing. etc. Based on experiment results, the cipher-images were robust to the image processing operations, since the modifications have little influence on low frequency DCT coefficients. The decrypted images can be still recognized well, although they are just like noised.

ACKNOWLEDGEMENT

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

REFERENCES

[1] 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.

[2] Jonathan M. Blackledge, Musheer Ahmad, and Omar Farooq (2010): *Chaotic Image Encryption Algorithm Based on Frequency Domain Scrambling*, Dublin Institute of Technology, 2010.

[3] Rinaldi Munir, "Algoritma Enkripsi Selektif Citra Digital dalam Ranah Frekuensi Berbasis Permutasi *Chaos*", Jurnal Rekayasa Elektrika, Jurusan Teknik Elektro Universitas Syiah Kuala, Banda Aceh, Edisi Oktober 2012 (*accepted*)

[4] Katherine Struss (2009): *A Chaotic Image Encryption*, Mathematics Senior Seminar, 4901, University of Minnesota, Morris.

Supported by IEEE Indonesia Section, IEEE APS/MTT Indonesia Joint Chapter, and IEEE Communication Society (Comsoc) Indonesia Chapter ISBN 978-602-8509-18-3

Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics (MICEEI), 28 November-1 December 2012, Makassar Golden Hotel (MGH), Makassar, Indonesia

Supported by IEEE Indonesia Section, IEEE APS/MTT Indonesia Joint Chapter, and IEEE Communication Society (Comsoc) Indonesia Chapter ISBN 978-602-8509-18-3