The University of Jember

INTERNATIONAL BASIC SCIENCE CONFERENCE

MATHEMATICS

ISBN:978-602-60569-5-5

Proceeding The 1st IBSC: Towards The Extended Use Of Basic Science For Enhancing Health, Environment, Energy And Biotechnology
ISBN: 978-602-60569-5-5

Image Encryption Technique Based on Pixel Exchange and XOR Operation

Kiswara A Santoso[1], Fatmawati[2], Herry Suprajitno[3]
[1] Mathematics Department, University of Jember, Indonesia
[2,3] Mathematics Department, Airlangga University, Indonesia
e-mail: kiswaras@gmail.com

Abstract—Recently the information system develops quickly, especially information system via internet. It's happened because the Internet can be used by anyone, anywhere and anytime. The information on the Internet has various types of data such as text, video, audio, and image/photo. Although we can access the Internet easily, but the data which transfered through internet isn't safe. It caused by hacker, someone who manipulate information so that data become different with the original. Many efforts have been done to make the data that transmitted over the Internet to be secure, for example make the coding, disguise or hide data into other media. In this paper we intend to present the results of research about image encryption techniques to increase the security of data (image) so that safe if the data is transfered via the internet. This encryption using symmetric-key. The key is 4 BIT or a real number between 0 15. This key will be processed by each pixel in the image using XOR operation. The next step the BIT of pixels are devided into two part, LSB (least significant bit) and MSB (Most significant bit). Both will be exchanged if the conditions have completed. We do that to get better results, that is file size of the image encryption is smaller than the original image. The results of this research are image encryption have significant differences with the original image, it can be proved by correlation between both images. Another advantage of this coding technique is the image encryption file size smaller than the original image file size so it can speed up of image transfer. Decode result of this coding technique is good enough, it can be seen from the mean square error (MSE) between the image encryption that has been restored to its original form and the original image. All the manufacturing process of encoding techniques have been simulated and analyzed using software MATLAB 2012a.

Keywords—BIT, Pixel, XOR

INTRODUCTION

The bitwise XOR operation is normally used as part of a more complex encryption algorithm. Numerous variations of the use of XOR in image encryption can be found in some literature or journal.

Vani Kumari (2015) makes an image coding techniques using a 128-bit hexadecimal key. Each 4-bit called subkey and every 8 bits called the session key. Before applying encryption using XOR operation, image was devided into equal number of blocks are decided by session key. Each block is taken and apply diffusion method (scramble in a zigzag manner). Then apply substitution method on each pixel value is modified with one of its 8 surrounding pixel. After applying the 16 iteration combine the blocks into single image [1].

The image encryption algorithm devided into three major groups. Pakshwar (2013) proposed image encryption using random scrambling and XOR operation. Affine transform that is based on shuffling the image pixels and they encrypting the resulting image using XOR operations. They used 32bit key that is good for practical [2].

Algorithm of Tamimi (2015) takes an image and a key as input. It performs variable – length key – dependent XOR encryption and applies byte substitution using lookup table called S-box. Different combinations of these two encryptions may be performed, where decryption performs the inverse of the applied steps in reverse order. In the XOR encryption operation of the algorithm, the image is regarded as a stream of bytes, and then it is devided into one dimensional blocks [3].

An image is defined as two dimensional function, f(x,y), where x and y are spatial coordinates, and the amplitude off at any pair of coordinates (x,y) is known as intensity of gray level of image at that particular point. The image is known as digital image when x, y, and the amplitude values of f are finite and discrete values. Processing of digital image by means of digital computer is done in the field of digital image processing. Adigital image constitutes a finite number of element, each of which has a particular location and a particular value. These elements are called picture element or image element or pixels. Pixels is the term most widely used to denote the element of a digital image [4].

The following table shown how the XOR operation transforms individual bits. Let A be a bit from the plain image and B be a bit from the key. The exclusive OR ($\oplus$) shows the resulting bit

Table 1. XOR operation individual bit

A	B	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

Pixel of the image can be converted into 8 binary digits (bits). The first to fourth bits called LSB (Least Significant Bit), where changes the value of the bit at this position does not have a real impact on the image [5]. The fifth to eighth bits called MSB (Most Significant Bit), where changes the value of the bit in this position give a real impact on the image [6].

The following figure shows the position of MSB and LSB to a bit value [7].

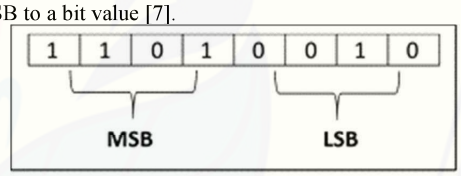

Fig 1. MSB and LSB Position

PROPOSED ALGORITHM

In this paper we propose image encryption algorithm base on pixel exchange. The key for encoding is real number between 0 – 15 or 4 bitwise. Bit positions that exchanged is formulated the following:

$t = (\text{key} \oplus LSB_{xy}) * (N/15) + (N \bmod 16)$
$temp = MSB_{xy}$
$MSB_{xy} = MSB_{xt}$
$MSB_{xt} = temp,$
where :
LSB_{xy} = LSB of pixel at (x,y) position
MSB_{xy} = MSB of pixel at (x,y) position
MSB_{xt} = LSB of pixel at (x,t) position
N = the number of horizontal pixel image
T = pixel position that exchanged
Following the illustrate of pixel exchange

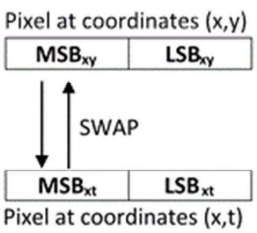

Fig 2. Illustration of pixel exchange

Encoding Algorithm
Input key
Load plain image (MxN size)
Convert pixel value into 8 bitwise
For i=1 to M
a. For j=1 to N
i. t =(key $\oplus$ LSB_{xy})*(N/15) + (N mod 16)
ii. Swap (MSB_{ij} , MSB_{it})

Decoding Algorithm
Input key
Load encrypt image (MxN size)
Convert pixel value into 8 bitwise
For i=M to 1 step -1
a. For j=N to 1 step -1
i. t =(key $\oplus$ LSB_{xy})*(N/15) + (N mod 16)
ii. Swap (MSB_{ij} , MSB_{it})

SIMULATION AND ANALYSIS

One way to measure the quality of the image that has been coded by visual observation. More and more elements of the image are missing then the better encoding algorithm. Aside from visual observation of, can also be observed quantitatively grayscale. The higher a pixel value changes, the encoding is said better. Changes in the value of the pixel can be seen from the maximum deviation, correlation coefficient, deviation irregular and long coding [8].

To analyze this method, suppose two image Carrot.jpg and Lena.jpg. When seen visually if both files encoded using keys 9 or 1001 is as follows:

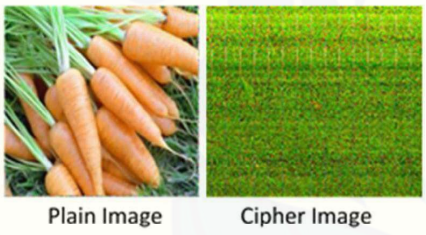

Fig 3. Visual observation of carrots image

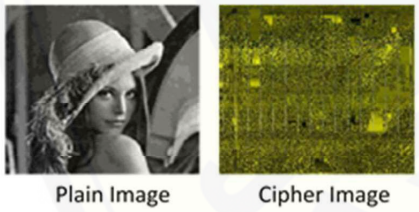

Fig 4. Visual observation of Lena image

From visual observation of Figures 3 and 4 above shows that the encoded image is difficult to be interpreted.

The maximum deviation of an image can be found by making the histogram of grayscale and calculate its area. The greater the deviation, the encoding area is said better. To find the area of the image histogram can be used formula: [9]

$$L = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i$$

L = The area of deviation
h_i = number of pixels that have different i
i = the value of the pixel

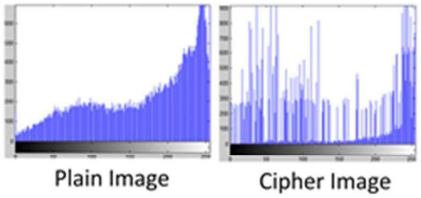

Fig 5. Histogram of carrots image

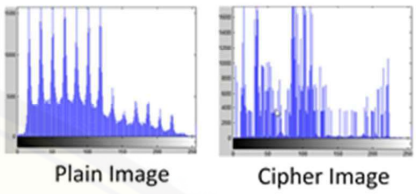

Fig 6. Histogram of Lena image

From histogram of Figures 5 and 6 above shows that an intensity encoded image more unequal than plain image, causing the image to be worse. The deviation of plain carrot is 68.6271, the deviation of cipher carrot is 70.6294. The deviation of plain Lena is 52.1668, the deviation of cipher Lena is 53.8946.

[5] The correlation coefficient in the image expressed how close the relationship between image pixels which is encoded and the original image. The formula to find the correlation coefficient between the original image and the image which is encoded is:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i$$

$$CC \quad \frac{cov(x,y)}{\sigma_x \sigma_y}$$

$$= \frac{\sum_{i=1}^{N} \frac{x_{i-E(x)}}{y_{i-E(y)}}}{\sqrt{\sum_{i=1}^{N}(x_{i-E(x)})^2}\sqrt{\sum_{i=1}^{N}(y_{i-E(y)})^2}}$$

x_i = the original image pixel at position i
y_i = pixel image encoding at position i
N = total pixels

From the analysis of the correlation coefficient is if the value of CC is getting smaller, it is said that the better encoding results. If CC = 1 then said both image identical or encoding fail. If CC = 0 then both image is different perfectly. The correlation coefficient of Carrot is 0.0262. The correlation coefficient of Lena is 0.1161. Simulation and analysis of the algorithm using software matlab 2012a

CONCLUSIONS

We proposed an algorithm of image encryption base on pixel exchange and XOR operation. We produced encrypted image by pixel exchange using XOR of MSB bitwise. The result of the encoding is good enough. It is proved by the small correlation coefficient value and deviation cipher image larger than the plain image, and the visual observations are very clear difference between the encoded image and the original image.

REFERENCES

[1] Kumari V., "Symmetric Diffusion-Double Substitution Based Image Encryption", International Journal of Advanced Reseach in Computer Science and Software Enginering, vol. 5, issue 8, pp. 888-892, 2015.

[2] Pakshwar, R., "Image Encryption Using Random Scrambling and XOR Operation", International Journal of Engineering R*eseach* & Technology, vol. 2, issue 3, pp. 1-7, 2013.

Proceeding The 1st IBSC: Towards The Extended Use Of Basic Science For Enhancing Health, Environment, Energy And Biotechnology
ISBN: 978-602-60569-5-5

[3] Tamimi A. "An Image Encryption Algorithm with XOR and S-box", International Conference Comp Vision and Pattern Recognition, pp. 166-169, 2015.

[4] Singh A., "DIP Using Image Encryption and XOR Operation Affine Transform", IOSR Journal of Computer Engineering, vol. 17, issue 2, pp. 07-15, 2015.

[5] Gangwar A., "Improved RGB-LSB Seganography Using Secret Key", Intrnational Journal of Computer Trend and Technology, vol. 4, issue 2, pp. 85-89, 2013.

[6] Purba, J V., "Implementasi Steganografi Kedalam File Sound (.wav) Dengan Modifikasi Jarak Byte Pada Algoritma LSB", Jurnal Dunia Teknologi Informasi, vol. 1, issue 1, pp. 50-55, 2012.

[7] Adak C., "Robust Steganography Using LSB-XOR and Image Sharing", International Journal on Computation and Comunication Advancement, pp. 97-102, 2013.

[8] Fhishawy`, "Quality of Encryption Measurement of Bitmap Image with RC6, MRC6, and Rijndael Block Cipher Algorithm", International Journal of Network Security, vol. 5, issue 3, pp. 241-251, 2007.

[9] Chang, "Gray-Level Image Encryption Scheme Using Full Phase Encryption and Phase Encoded Exclusive OR Operation", OPTICAL REVIEW, vol. 11, issue1, pp. 34-37, 2004.