Image Scrambling Using One Time Pad with Linear Congruent Key Generator

Imam Saputra

Department of Computer Science STMIK Budi Darma, North Sumatera, Indonesia

Abstract – With the changing of the times, more and more moments can be photographed. Digital imagery stores a lot of information through visual display. Many people perpetuate the things that are personal in the form of digital imagery, with so many files in the form of digital imagery that is private and not for publication. With the development of cloud computing systems, every image recorded through the smartphone will be synchronized with the online storage service provider. This has many advantages, such as users do not have to worry about the damage to storage devices that exist in their gadgets. But the disadvantage of this system is that if an account falls into the hands of an unauthorized person then photographs containing this personal information may be published by an unauthorized person, of course this will be very detrimental. One solution that can be used is to randomize the original image so that its visual appearance will not be like the actual visual display. One way that can be used for image randomization is by cryptographic techniques. The one time pad algorithm is a very powerful classical cryptographic algorithm and can not be solved by cryptanalis until now. One disadvantage of a one time pad algorithm is the key length must be the same as the length of the plaintext. This makes the algorithm unused because it is less practical in its key usage. To overcome this required a key generator that could generate randomly generated locks ie a linear congruent generator, thus the key length must be equal to the length of the plaintext can be generated only with a few variables. In this way, image randomization can be done with a strong and practical cryptographic algorithm.

Keywords - Image Scrambling, One Time Pad, Linear Congruent Generator

1 INTRODUCTION

The use of smart phones has become a necessity in human life. Almost all smartphones are equipped with tools to record images or commonly referred to as cameras. Every day there are many moments that can be captured through smart phone cameras because of its practical use and have good quality. Storage space capacity is also not a problem because every smart phone get online photo storage facility, so if there is damage to the storage device on the smart phone device is still available backup of the photo in online storage. The problem with this facility is that if the account falls to an unauthorized party, then a photo that is not for publication may be published by an unauthorized person so that it is very harmful.

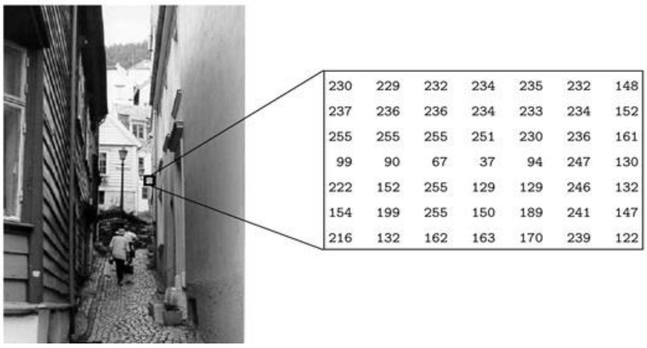
Digital imagery has a very rich visual display of information. Events captured through photos will be very similar to the original. To secure visual information contained in the digital image can be done randomization of pixel values so that the visual appearance seen by the human eye is not a visual display actually. This is very useful for securing visual information especially on visual information that is private and not for publication. One way that can be done is to scramble the visual information on the image with one of the cryptographic algorithms.
One time pad is a classical cryptographic algorithm that is known to be very powerful, so it can not be solved by cryptanalis. One characteristic of a one time pad algorithm is the key length must be the same as the length of the plaintext. This results in the one time pad algorithm being less practical in its implementation because it requires the length of the key to be equal to the length of the plaintext. To overcome this required a key generator, one of the algorithms that can be used to generate keys randomly is a linear congruent generator, thus the key length must be equal to the length of the plaintext can be generated only with a few variables. In the process of digital image randomization, the key length must be equal to the number of pixels contained in the image to be randomized.

2 THEORY

2.1 Digital Image

Digital imagery is a two-dimensional image representation as a limited set of digital values, known as picture or pixel elements [1]. Image is another term of the picture as one of the multimedia component that plays a very important role as a form of visual information. The image has characteristics that are not owned by text data, ie image rich in information. Image is a two-dimensional function that represents some characteristics such as the brightness or color of a scene and can be defined as a two-dimensional function f (x, y) where (x, y) the projection position and f (x, y) define the brightness at that point.

Image processing requires images in digital form. For that required the process of digitization, each inserted images taken samples and quantized with some techniques [2]. Digital imagery consists of elements called picture elements, image elements and pixels. The pixel is the smallest part of an image [6]. Digital imagery is divided into several types based on the color depth of the binary image, grayscale image (8 bits), color image (24 bits) and color image (32 bits). For grayscale images (8 bits) then the value for a pixel is represented by 8 bits of a binary number with a minimum value of 0 and a maximum value of 255.



230	229	232	234	235	232	148
237	236	236	234	233	234	152
255	255	255	251	230	236	161
99	90	67	37	94	247	130
222	152	255	129	129	246	132
154	199	255	150	189	241	147
216	132	162	163	170	239	122

Fig 1. 8 Bit Grayscale Image

2.2 Image Scrambling

The main purpose of digital image randomisation is to hide picture information by means of meaningful image transforms into meaningless or non-conflicting images to increase the power to withstand attacks and to improve security [3]. Image scrambling (encryption) is a good method to provide security to image data in making images visually unreadable and also difficult to decrypt by unauthorized users [4]. Digital image encryption uses two basic methods of replacing pixel values or displacement of pixel values, so it will be difficult to recognize by unauthorized parties [5].

The essence of image randomization is to reduce the correlation of the pixel position and the correlation of the pixel value until it becomes irrelevant. The process of randomizing the image can be regarded as a process of uncertainty improvement, as well as the process of adding the amount of image information. The correlation of natural image pixels has the greatest number in blocks and uncertainties.

2.3 Cryptography

Cryptography is a science used to maintain the confidentiality of a data, using certain methods so that the data can only be read by people who are entitled to the data. In maintaining data confidentiality, cryptography transforms the original data (plaintext) into encoded data (cipherteks). This process is called the encryption process. While the process of converting the encoded data (cipherteks) into the original data is called the decryption process. Cryptography can be classified into two categories:

a. Shared Key Cryptography
b. Public Key Cryptography

Shared Key Cryptography is also often called symmetric key cryptography or private key cryptography or a secret key because the key used in the encryption and decryption process is the same [6].

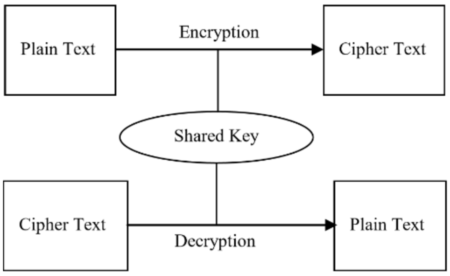


Fig. 2 Shared Key Cryptography

Public Key Cryptography is also often called asymmetric key cryptography that uses different keys on the process of encryption and decryption. The private key is only used for the encryption process. And the public key is used during the decryption process.

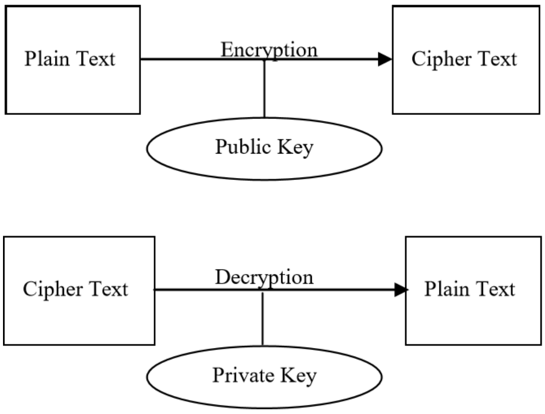


Fig. 3 Public Key Cryptography

2.4 One Time Pad

One time pad algorithm requires a key that is only used once and key is a collection that contains a random circuit [7]. One time pad is a cryptographic algorithm that is very easy to learn. This algorithm is also known as vernam cipher. The one time pad algorithm is a shared key cryptograhy algorithm because the keys are used at the same time encryption and decryption. The things to be aware of in the selection of keys are that the selection of keys must be completely random so it is not easy to guess and the key length should be the same length as the plaintext. One time pad is a encryption stream cipher that was discovered in 1917 by Major Joseph Mauborgne as a refinement of the vernam cipher to produce perfect security [8]. The encryption rules used are the same as the vigenere cipher encryption rules. One key is used to encrypt one plaintext [7].

The encryption and decryption process of one time pad can be represented in mathematics as follows:

Encryption : Ci=(Pi+Ki) mod 26
Decryption : Pi=(Ci-Ki) mod 26
Where : Ci = Ciphertext
Pi = Plaintext
Ki = Key

If one time pad is applied to randomize the pixel value of a digital image then the value that can be used is between 0-255, so if it is represented mathematically as:
Encryption : $C_i = (P_i + K_i) \bmod 256$
Decryption : $P_i = (C_i + K_i) \bmod 256$

2.5 Linear Congruent Generator

Random number generators are devices designed to produce numerical sequences or symbols that do not have any pattern [9]. The Pseudo Random Number Generator (PRNG) is also known as a deterministic random bit generator that is used to generate a sequence of numbers that approximates the nature of random numbers. The sequence is not really random as it is entirely determined by a relatively small set of initial values [10]. Linear Congruent Generator is a very basic random number generator algorithm. Here is an equation for generating random numbers.

$x_n=(ax_{n}-_1 + b) \bmod m$

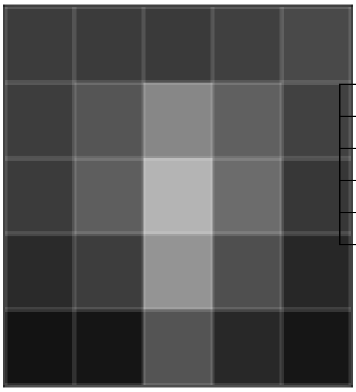
Where: xn = The random number of the series

$X_{n}-_1$ = Previous random number
a = multiplier
b = increment
m = modulus

x_0 is a generator key or also called a feed. Linear congruent generator has a period not greater than m and in fact many cases are less than that, the advantages of linear congruent generator is at a speed that requires only a bit of bit operation.

3 RESULT AND DISCUSSION

The input or input in the randomization of an image is the pixel value of a digital image, in which case the input or input is a grayscale image measuring 5 x 5 pixels. To get or extract the pixel value of the image is used software Matlab R2013a.



48	41	39	42	48
46	58	134	74	44
46	37	142	88	45
26	42	152	72	20
15	20	44	26	14

Fig 3. Digital Image Input 5x5 Pixel

To generate a series of keys equal to input or input lengths, a 25-key key will be generated using a linear congruent generator with values X0 = 15, a = 3, b = 17 and m = 255.

Table 1. Linear Congruent Key Generator

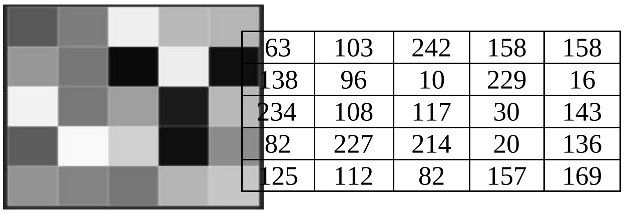
Order	**Process**	**Result**
X_0	-	15
X_1	(15 * 3 + 17) mod 255	62
X_2	(62 * 3 + 17) mod 255	203
X_3	(203 * 3 + 17) mod 255	116
X_4	(116 * 3 + 17) mod 255	110
X_5	(110 * 3 + 17) mod 255	92
X_6	(92 * 3 + 17) mod 255	38
X_7	(38 * 3 + 17) mod 255	131
X_8	(131 * 3 + 17) mod 255	155
X_9	(155 * 3 + 17) mod 255	227
X_{10}	(227 * 3 + 17) mod 255	188
X_{11}	(188 * 3 + 17) mod 255	71
X_{12}	(230 * 3 + 17) mod 255	230
X_{13}	197 * 3 + 17) mod 255	197
X_{14}	(98 * 3 + 17) mod 255	98
X_{15}	(56 * 3 + 17) mod 255	56
X_{16}	(185 * 3 + 17) mod 255	185
X_{17}	(62 * 3 + 17) mod 255	62
X_{18}	(203 * 3 + 17) mod 255	203
X_{19}	(116 * 3 + 17) mod 255	116
X_{20}	(110 * 3 + 17) mod 255	110
X_{21}	(92 * 3 + 17) mod 255	92
X_{22}	(38 * 3 + 17) mod 255	38
X_{23}	(131 * 3 + 17) mod 255	131
X_{24}	(155 * 3 + 17) mod 255	155

3.1 Encryption Process

The encryption process uses a one time pad algorithm with keys that have been generated by linear congruent generator, the process is presented in the following table:

Table 2. Encryption Process

Pixel Position	Process	Result
$X_{(1,1)}$	(48+15) mod 255	63
$X_{(1,2)}$	(41+62) mod 255	103
$X_{(1,3)}$	(39+203) mod 255	242
$X_{(1,4)}$	(42+116) mod 255	158
$X_{(1,5)}$	(48+110) mod 255	158
$X_{(2,1)}$	(46+92) mod 255	138
$X_{(2,2)}$	(58+38) mod 255	96
$X_{(2,3)}$	(134+131) mod 255	10
$X_{(2,4)}$	(74+155) mod 255	229
$X_{(2,5)}$	(44+227) mod 255	16
$X_{(3,1)}$	(46+188) mod 255	234
$X_{(3,2)}$	(37+71) mod 255	108
$X_{(3,3)}$	(142+230) mod 255	117
$X_{(3,4)}$	(88+197) mod 255	30
$X_{(3,5)}$	(45+98) mod 255	143
$X_{(4,1)}$	(26+56) mod 255	82
$X_{(4,2)}$	(42+185) mod 255	227
$X_{(4,3)}$	(152+62) mod 255	214
$X_{(4,4)}$	(72+203) mod 255	20
$X_{(4,5)}$	(20+116) mod 255	136
$X_{(5,1)}$	(15+110) mod 255	125
$X_{(5,2)}$	(20+92) mod 255	112
$X_{(5,3)}$	(44+38) mod 255	82
$X_{(5,4)}$	(26+131) mod 255	157
$X_{(5,5)}$	(14+155) mod 255	169



63	103	242	158	158
138	96	10	229	16
234	108	117	30	143
82	227	214	20	136
125	112	82	157	169

Fig 5. Encryption Result

After performing the encryption process the pixel value of the input image is shown in figure 5.

3.2 Decryption Process

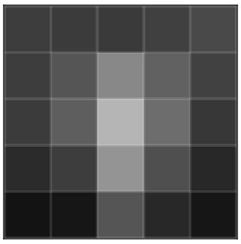
The decryption process is performed using the same key because the one time pad algorithm is a symmetric key cryptography algorithm in which the key for encryption and decryption is the same, the process is presented in the following table:

Table 3. Decryption Process

Pixel Position	Process	Result
$X_{(1,1)}$	(63-15) mod 255	63
$X_{(1,2)}$	(103-62) mod 255	103
$X_{(1,3)}$	(242-203) mod 255	242
$X_{(1,4)}$	(158-116) mod 255	158
$X_{(1,5)}$	(158-110) mod 255	158

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 8-14

Pixel Position	Process	Result
$X_{(2,1)}$	(138-92) mod 255	138
$X_{(2,2)}$	(96-38) mod 255	96
$X_{(2,3)}$	(10-131) mod 255	10
$X_{(2,4)}$	(229-155) mod 255	229
$X_{(2,5)}$	(16-227) mod 255	16
$X_{(3,1)}$	(234-188) mod 255	234
$X_{(3,2)}$	(108-71) mod 255	108
$X_{(3,3)}$	(117-230) mod 255	117
$X_{(3,4)}$	(30-197) mod 255	30
$X_{(3,5)}$	(143-98) mod 255	143
$X_{(4,1)}$	(82-56) mod 255	82
$X_{(4,2)}$	(227-185) mod 255	227
$X_{(4,3)}$	(214-62) mod 255	214
$X_{(4,4)}$	(20-203) mod 255	20
$X_{(4,5)}$	(136-116) mod 255	136
$X_{(5,1)}$	(125-110) mod 255	125
$X_{(5,2)}$	(112-92) mod 255	112
$X_{(5,3)}$	(82-38) mod 255	82
$X_{(5,4)}$	(157-131) mod 255	157
$X_{(5,5)}$	(169-155) mod 255	169



48	41	39	42	48
46	58	134	74	44
46	37	142	88	45
26	42	152	72	20
15	20	44	26	14

Fig 6. Decryption Result

It can be seen that the relationship between the original image and the image after being encrypted or after being scrambled has a very pseudo relation so that the original visual information can not be read by unauthorized parties. So if the image has a secret visual information can not be known by unauthorized parties. Key randomness affects the relationship between the original image with the image of the encrypted image or the result of the randomization. If applied to the image with the actual size then the results can be seen in figure 7 below. Encryption and decryption process is done using Matlab R2013a software.

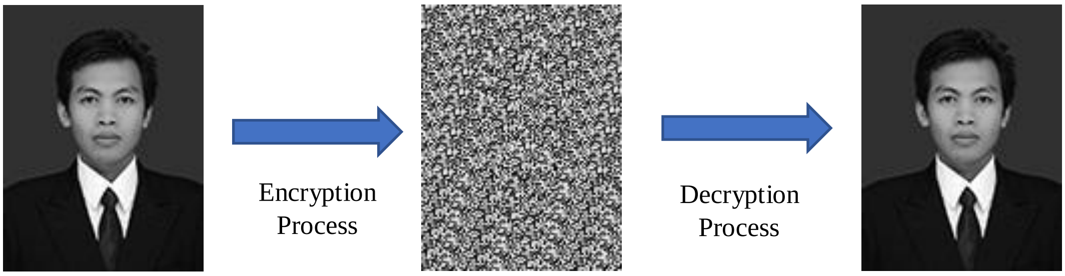


Fig 7. Result in Original Image Size

4 CONCLUSION

This study discusses randomization of images using one time pad algorithm which is a very powerful algorithm and very difficult to solve by cryptanalis if it has a long and random key. Using a generated key using a linear congruent random generator will generate a random key and the length can be adjusted to the size of the image to be randomized. By using a random number generator it is not necessary to remember a long and random key, which is necessary only to remember the variables used to generate a random number that is key. Once randomized the visual information from the original image will not be understood and after the decryption then the visual information on the image will return as before.

REFERENCES

[1] M. Bhat, "Digital Image Processing," Int. J. Sci. Technol. Res., vol. 3, no. 1, pp. 272–276, 2014.

[2] B. Shinde, D. Mhaske, and A. R. Dani, "Study of Image Processing , Enhancement and Restoration," vol. 8, no. 6, pp. 262–264, 2011.

[3] Z. Liehuang, L. Wenzhuo, L. Lejian, and L. Hong, "A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequences," J. Comput. Sci., vol. 6, no. 8, pp. 125–130, 2006.

[4] H. Kekre, T. Sarode, and P. Halarnkar, "Image Scrambling using R-Prime Shuffle," … J. Adv. Res. …, pp. 4070–4076, 2013.

[5] D. R. Ahmed, "Simple Image Scrambling Algorithm Based on Random Numbers Generation," vol. 5, no. 9, pp. 434–438, 2015.

[6] Y. Rajput, "An Improved Cryptographic Technique to Encrypt Text using Double Encryption," Int. J. Comput. Appl., vol. 86, no. 6, pp. 975–8887, 2014.

[7] M. Iqbal, M. Akbar, S. Pane, A. Putera, and U. Siahaan, "SMS EncryptionUsing One-Time Pad Cipher," vol. 18, no. 6, pp. 54–58, 2016.

[8] Zaeniah and B. E. Purnama, "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm," Int. J. Adv. Comput. Sci. Appl., vol. 6, no. 9, pp. 292–297, 2015.

[9] M. E. S and P. Arulmozhi, "Linear Congruential Generator for LUT-SR Architecture," vol. 2, no. 3, pp. 97–102, 2014.

[10] M. Mishra and P. D. Scholar, "Text Encryption Algorithms based on Pseudo Random Number Generator," vol. 111, no. 2, pp. 1–6, 2015.