LUC Algorithm in Visual Cryptography

Ratnadewi1*, Christian Dio Alpha G2, Darmawan Napitupulu1, Heri Nurdiyanto3, Nuning Kurniasih5, Abdurrozaq Hasibuan6, Ahmad Senggeng4, Rosida Tiurma Manurung6, Indrya Mulyaningsih9, Rabi Ralah10, Castaka Agus Sugianto11 and Dahlan Abdullah12

1,2Department of Electrical Engineering, Universitas Kristen Maranatha, Bandung, Indonesia
3Research Center for Quality System and Testing Technology, Indonesian Institute of Sciences, Banten, Indonesia
4STMIK Dharma Wacana, Indonesia
5Faculty of Communication Sciences, Library and Information Science Program, Universitas Padjadjaran, Bandung, Indonesia
6Universitas Islam Sumatera Utara, Indonesia
7University of 45, Surabaya, Indonesia
8Graduate Program in Scientific Psychology, Universitas Kristen Maranatha, Bandung, Indonesia
9Department of Education, Institut Agama Islam Negeri Syekh Nurjati Cirebon, Indonesia
10School of Computer and Communication Engineering, Universiti Malaysia Perlis, Kedah, Malaysia
11Politeknik Negeri Banda Aceh, Aceh, Indonesia
12Department of Informatics, Universitas Malikussaleh, Aceh Utara, Indonesia

*ratnadewi.bandung@gmail.com

Abstract. Nowadays, messaging technology in digital data form more often used and not less messages that confidentially wanted. Then it should be modified so that can be understood only by the sender and the intended recipients. All of this system can be realization by using cryptography. LUC algorithms are introduced by Smith and Lennon in 1993. LUC algorithm is an algorithm that based on the use of Lucas sequence (specific arithmetic operations derived from Lucas row) that rarely used to enhance the security of the messages. In this research, LUC algorithm is combined with visual cryptography to process the encryption and the description of a colored image. Four different images were used in the trial here. The performance of the system is assessed using Structural similarity (SSIM) which has an assessment similar to human eye. If the image quality is the same as the original image, then the SSIM value is one. Whereas if the quality of decryption image is very different from the original image then the value of SSIM is zero.

1. Introduction
Visual cryptography is used to share one image into some share image. The share image did not same with the original image, the share image looks like a rain water image. The share image can be two, three, or more. This share image must be combining together to have the original image. Visual
cryptography first published by Naor Shamir(1) i.e. sharing one original image into two shared images.

There are many method development with researcher until now, among them (2) ElGamal algorithm use in visual cryptography, RSA Algorithm, improvement of flip (2,2) image(3). The decryption image has a good image like the original image before encryption. The application can be used for healthy cases (4) or for text similarity cases (5).

On the visual cryptography when sharing the original image into a shared image then the person who received only one of the share images cannot know the original image, this will be proven in the paper here. If one of the shared images is decrypted, the decrypted image will not show the same information as the original image. This will be evidenced by performance measurement through SSIM.

In this paper to improve security then the classical cryptography visuals are combined with classical cryptography so the combination of these two methods enhances the security of the transmitted images. There are many algorithm cryptography i.e. DES (6), 3DES, AES(7), RSA, etc. In this paper we used LUC algorithm in visual cryptography.

2. Method
The process encryption can be described: first a secret colour image is parsed into red, green, and blue components and then each component would be encrypted with LUC algorithm and public key. After encrypted the cipher image will share to share A and share B.

In the decryption process the share A and share B would be parsed into each component into red, green, and blue components. Then the next process is combining each component share A with Share B. After that we proceed with LUC decryption algorithm to have image. This process can be showed in Figure 1.

2.1 LUC Algorithm
The LUC algorithm is an asymmetric cryptographic algorithm where two different key public key and private key. When a public key can be distributed for all user, but private key is secret only for one user. These algorithms were first discovered by Peter J. Smith and Michael J.J. Lennon. The LUC algorithm is an algorithm based on the use of the Lucas function that is rarely used to improve message security. We denote the public key with \( e \), private key with \( d \), the image original with \( P \), the cipher image with \( C \). The row of Lucas to \( n \), \( T_n \), is defined as (8)(9):

\[
T_n \equiv P T_{n-1} \pmod{n} - T_{n-2} \equiv C
\]

The LUC algorithm consists of three processes: first, the process of forming the key, the second is process of encryption and the third is process of decryption.

The first generation of the process: first choose any prime \( p \) and \( q \) with the condition of \( p \times q < 255 \), because the component red image value, component green image value, and component blue image value only covers 0-255 intensity value. The results of decryption of chipper image will not exceed the value \( p \times q \). The second process count \( N \) with this equation (8)(9):

\[
N = p \times q
\]

The third process is to select the encryption key \( e \) which is a relatively prime random number to \( p - 1 \), \( q - 1 \), \( p + 1 \), \( q + 1 \). Then calculate the value of (9) (10):

\[
R(N) = \text{LCM}[(p + 1)(q + 1)]
\]

The fourth calculate the \( d \) value with the formula (9) (10):

\[
ed \equiv 1 \pmod{R(N)}
\]
Then there will be two keys are public key \((e, N)\) and private key \((d, p, q)\).

2.2 Encryption process

In the encryption algorithm, the key used is the public key \((e, N)\). The encryption function will calculate the \(n\)th term of the lineup of Lucas with index \(n\) is public key \(e\) and \(P\) is image original. So for encrypt image original \(P\) and public key LUC \((e, N)\) expressed as (9) (10):

\[
C \equiv T_e(P, 1) \mod N \tag{5}
\]

The encryption process produces cipher text \(C\).

On the encryption process, we are calculating the value of encryption with the formula (5). The variable \(s\) as a multiplier of formula (6). The value of \(s < 255/p\) is the highest pixel value in RGB color description. The value 255 should be divisible by \(255 < p \leq (2 \times 255)\) so that the result does not exceed the intensity value color. The new formula \(C_1\) is

\[
C_1 \equiv s \times T_e(P, 1) \mod N \tag{6}
\]

The second cipher image formula \(C_2\) is the difference of \(C\) and \(C_1\)

\[
C_2 = [T_e(P, 1) \mod N] - [s \times T_e(P, 1) \mod N] \tag{7}
\]

or

\[
C_2 = (1-s) \times [T_e(P, 1) \mod N] \tag{8}
\]
The formula $C_1$ and $C_2$ is the formula that will form share image A and share image B.

### 2.3 Decryption process

In the decryption algorithm the key used is the private key $d$. With the following stages: first combine the value of Share A and Share B by the formula:

$$C = C_1 + C_2 \quad (9)$$

Count decryption image $M$ with formula (9) (10):

$$M \equiv T_d(C, 1) \mod N \quad (10)$$

### 3. Result and Discussion

There are four images we use in this testing process that is bird, owl, t-rex, and data images. Figure 2 show original image bird. The process encryption need 4.314 seconds until we accept share image A and share image B. The decryption image can be seen in Figure 3, with decryption time process 28.939 seconds and SSIM value is 1. The value $SSIM$ can be identified with the human eye, the value 1 means that the decryption image is the same as original image.

Figure 4 shows the share image A and Figure 5 shows the share image B. Figure 6 shows the decryption image if in process decryption only one share image A accepted. The SSIM value is 0.038 and decryption time is 27.657 seconds. In Figure 7 the decryption image if only one share image B use in process decryption. The SSIM value is 0.0272 and decryption time is 27.443 seconds. If the SSIM value towards to zero then the comparable image is not the same.
Figure 6. The decryption image if only share image A is accepted.

Figure 7. The decryption image if only share image B is accepted.

Figure 8 shows the graphics of encryption processing time and decryption time with two share images, one share image A, and one share image B. We can see that decryption process take a long time than encryption time.

Figure 8. The graphics of processing encryption time and decryption time.

Figure 9 shows the graphics of SSIM decryption with two share image, only one share image A, and only one share image B. This graph proves that decryption with two share images will produce the same image with the original image, whereas if only one share is obtained then the decryption process will produce images very much different from the original image.
4. Conclusion
Visual cryptography experiments on colour digital image with LUC algorithms can be implemented. The quality of the decrypted image is the same as the image before it is encrypted (it can be seen from the SSIM testing that is worth one). If only received one share and decrypted looks very bad results (can be seen the value of SSIM is close to zero).

References
1. Naor M, Shamir A. Visual Cryptography. In: Proc Adv Cryptol: Eurprocrypt’94, LNCS, 1994, vol 950, pp 1–12. 1994. p. 1–12.
2. Kacaribu AES, Ratnadewi. Multiplying cipher images on visual cryptography with ElGamal algorithm. In: 2nd International Conference on Information Technology, Computer, and Electrical Engineering: Green Technology Strengthening in Information Technology, Electrical and Computer Engineering Implementation [Internet]. Semarang, Indonesia: IEEE; 2016. p. 159–62. Available from: http://ieeexplore.ieee.org/document/7437790/
3. Ratnadewi R, Adhie RP, Comput Math Eng Appllications [Internet]. 2016;7(3):213–23. Available from: http://journal.binus.ac.id/index.php/comtech/article/view/2501
4. Mesran A, Syahbandi M, Suginam S, Kurniasih N, Gs AD. Expert System for Disease Risk Based on Lifestyle with Fuzzy Mamdani. Int J Eng Technol. 2018;7(2.3):88–91.
5. Kurniasih NM, Tawan MD, Siregar YH, D, Sari P, et al. Latent Semantic Indexing for Indonesian Text Similarity. Int J Eng Technol. 2018;7(2.3):73–7.
6. Ratnadewi, Adhie RP, Hutama Y, Saleh Ahmar A, Setiawan MI. Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method for Communication System Based Near Field Communication (NFC). J Phys Conf Ser. 2018;954(1).
7. Ratnadewi R, Adhie RP, Hutama Y, Christian J, Wijaya D. Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system. World Trans Eng Technol Educ [Internet]. 2017;15(2):178–83. Available from: http://www.wiete.com.au/journals/WTE&TE/Pages/Vol.15, No.2 (2017)/15-Ratnadewi.pdf
8. Ali Z, Ahmad A. Implementation of parallel algorithm for LUC cryptosystems based on addition chain by a message passing interface. J Theroretical Appl Inf Technol [Internet]. 2016;92(1):190–9. Available from: www.jatit.org/volumes/Vol92No1/22Vol92No1.pdf
9. Koval A. On Lucas Sequences Computation. Int J Commun Netw Syst Sci. 2010;2010(December):943–4.
10. Ali ZM, Makhzoum NMA. Computation of private key based on Divide-By-Prime for luc cryptosystems. J Comput Sci. 2012;8(4):523–7.

Retracted