A Single, Triple Chaotic Cryptography Using Chaos in Digital Filter and Its Own Comparison to DES and Triple DES

Reatrey Pich
International College
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: reatrey.pich@gmail.com
/59610026@kmitl.ac.th

Sorawat Chivapreecha
Department of Telecommunication
Engineering, Faculty of Engineering
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: sorawat@telecom.kmitl.ac.th

Jaruwit Prabnasak
International College
King Mongkut's Institute of Technology
Ladkrabang, Bangkok 10520, Thailand
Email: kpjaruwi@kmitl.ac.th

***Abstract*—The Data Encryption Standard (DES) of the multimedia cryptography possesses the weak point of key conducting that is why it reaches to the triple form of DES. However, the triple DES obtains the better characteristic to secure the protection of data to against the attacks, it still contains an extremely inappropriate performance (speed) and efficiency in doing so. This paper provides the effective performance and the results of a single and triple chaotic cryptography using chaos in digital filter, compare to DES and triple DES. This comparison has been made pair-to-pair of single structure respectively to the triple form. Finally the implementation aspects of a single chaotic cryptography using chaos in digital filter can stand efficiently as better performance speed with the small complexity algorithm, points out the resemblances to DES and triple DES with the similar security confirmation results without reaching to the triple form of the structure. Simulation has been conducted using Matlab simulation with the input of grayscale image.**

Keywords—Cryptography; DES; Triple DES ; Chaos in Digital Filter

I. INTRODUCTION

Cryptography is one of techniques of security concern in data transmission. It covers various aspects such as security, compression efficiency, encryption efficiency and format compliance. There are many data encryption algorithms which have been widely used like DES, triple DES, AES or IDEA, but in the point of multimedia data is different from text because multimedia data has high redundancy, so it produced non appropriate cipher-image [1]. For DES using Logistic map can make the cipher-image to be the stochastic noise to against the attacks, but it contains of high complexity because of round keys randomization [2]. The high security of encrypted image with three different round keys accompanied by chaotic properties have made cipher-image to be secure strongly too but it gave the same problem of complexity of making cipher image to be elliptic curve [3]. Same as Triple DES which makes the performance issues three time worse compare to its single form. Chaos in digital filter produces the nonlinear behavior and unstable system to make the cipher-image possess security by matching with overflow nonlinearity function [4].

II. CHAOTIC IN DIGITAL FILTER AND DES

A. Chaotic In Digital Filter

Chaotic cryptography is known as the dynamic system and using chaos in digital filter has produced the unstable system and nonlinear behavior to make the system is more profitable by involved with mathematic operation and overflow function [4-5]. During the process all-pole IIR filter function as encryption engine while its inverse form as all-pole FIR filter will work as decryptor. The detail of all-pole IIR filter is in the figure. 1 and equation (1-4).

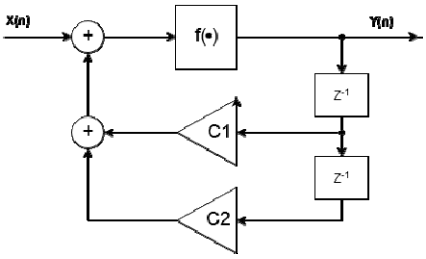


Fig. 1 All-pole IIR filter in second order

$$y(n) = x(n) + C_1 y(n-1) + C_2 y(n-2) \quad (1)$$

$$H(z) = \frac{y(z)}{x(z)} = \frac{1}{(1 - C_1 z^{-1} - C_2 z^{-2})} \quad (2)$$

$$f(x) = [(x+1) \bmod 2] - 1 \quad (3)$$

$$y(n) = f\{x(n) + C_1 y(n-1) + C_2 y(n-2)\} \quad (4)$$

In order to make sure that system is unstable and conducts with nonlinear behavior to produce the chaos inside the system, the coefficients are at least one is outside the stable triangle and system is worked through the overflow function [6].

978-1-5386-2615-3/18/$31.00 ©2018 IEEE

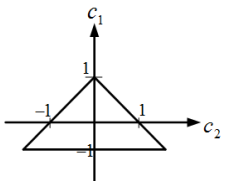


Fig. 2. The stable triangle.

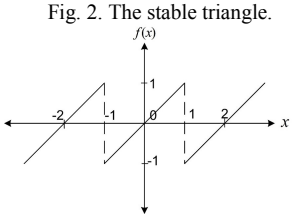


Fig. 3. The characteristic of overflow function.

B. *Data Encryption Standard (DES)*

DES is a 64 bits block cipher which work with 64 bits of data per time. It uses 64 bits key input, but only 56 bits of the key will be used inside the operation. In this technique it is used as iteration process that is known as Round. The whole process consist of 16 rounds. More detail is shown in figure. 4.

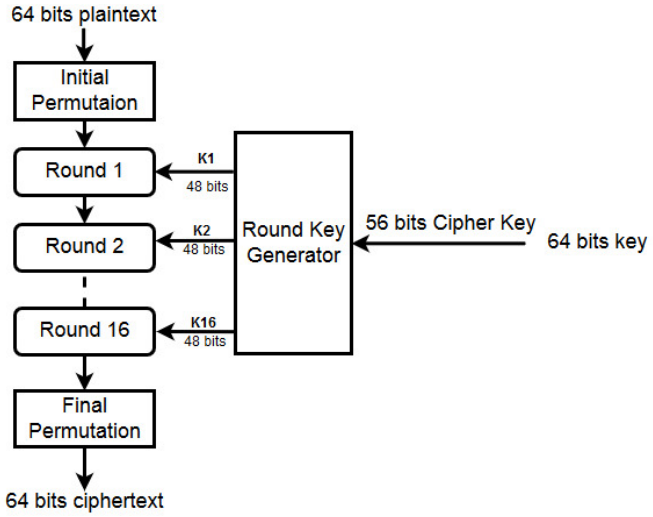


Fig. 4. Block diagram of Data Encryption Standard

For the structure of triple DES is the combination of three time of single DES by using the key bundle in order to generate K_1, K_2 and K_3. The detail of encryptor is show as below:

$$\text{Cipher-Image} = E_{K3}(D_{K2}(E_{K1}(\text{Plain-Image})))$$

For the decryptor is the inverse form of the encryptor only by exchanging the Encrypted process to Decrypted process and Decrypted process to Encrypted process.

III. The Proposed Structure

A. *Single form of Chaotic cryptography*

The proposed structure for data encryption using chaos in digital filter is composed by two main parts. First is the key generator which is made up with three all-pole IIR filters of input of 16 characters (128 bits). Second is the encryption engine which uses only one all-pole IIR filter to perform the process. The system provides the value as key sensitivity and high security confirmation [7]. The detail is shown in Fig. 5.

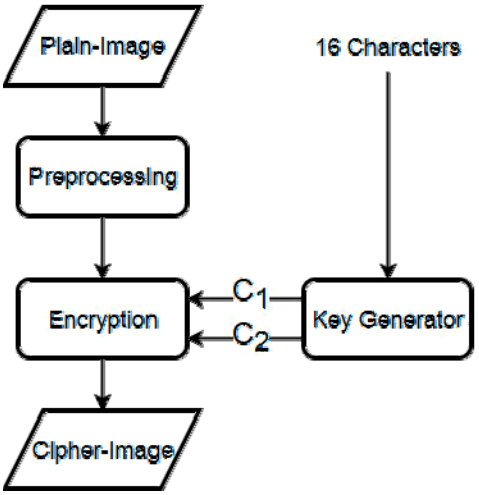


Fig. 5 The structure of single form of chaotic cryptography.

B. *Triple form of Chaotic cryptography*

For its triple form is made as the concept of triple DES and followed the structure of single chaotic cryptography. But for the coefficients of each filters of encryption engine are produced by different sub key generators which have different made up coefficients but the same input of 16 characters. The strong security over the single form is it has more initialed values than the single. The detail is in Fig. 6.

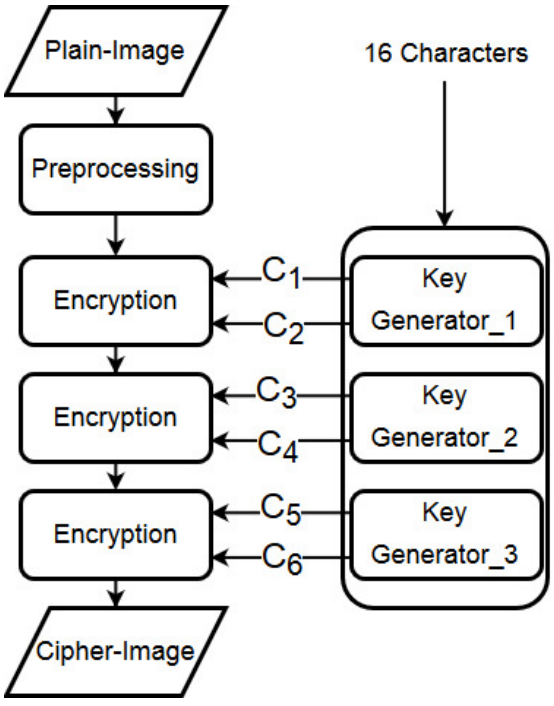


Fig. 6 The structure of triple form of chaotic cryptography.

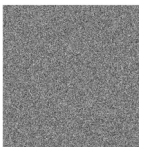
IV. THE EXPERIMENT

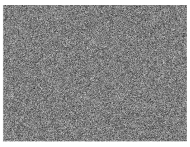
For the experiment, the input data are the gray scale image. Inside the paper, three images have been selected for testing the security and results analysis. Input and output of chaotic cryptography are shown respectively:

(a) Lenna image

(b) Baboon image

(c) Pepper image





(d) Lenna cipher-image (e) Baboon cipher-image (f) Pepper cipher-image

A. The proposed structure results

In order to confirm about the security and sensitivity inside the cipher-image to make sure our system is qualified enough to use, there are some main factors to be considered:

- Key Space, Key Sensitivity and Plaintext Sensitivity: the values that can confirm that our system can against the attacks such as brute force attack which is widely known. Moreover, to make sure our system is sensitive to the key, key sensitivity is the main factor to be considered.

TABLE I. KEY SPACE

Key Length (bits, Char)	Algorithm	Key Space	Time To Brute Fore
128 , 16	**Single form of proposed technique**	4.4 x 10^{38}	4.4 x 10^{31} years
57, 7	DES	7.2 x 10^{16}	13 years 91 days
128, 16	**Triple form of proposed technique**	4.4 x 10^{38}	4.4 x 10^{31} years
168, 21	Triple-DES	3.7 x 10^{50}	3.4 x 10^{41} years

To define key sensitivity the formula below is used:

$$Ks = \frac{100\%}{2MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} K_1(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} K_2(i,j)\right) \quad (5)$$

where $K_1(i,j)$ and $K_2(i,j)$ are defined by

$$K_k(i,j) = \begin{cases} 0 & \text{if } F(i,j) = F_k(i,j) \\ 1 & \text{if } F(i,j) \neq F_k(i,j) \end{cases} \quad (6)$$

where F(i,j) and $F_k(i,j)$ are the cipher-images with different one bit of the key input.

TABLE II. KEY SENSITIVITY

Image	Key Sensitivity (Ks) %	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	99.9999	99.9998
Baboon	99.9998	99.9998
Pepper	99.9997	99.9997

To define Plaintext sensitivity, Number of Pixel Change rate of cipher-image (NPCR) and Unified average changing intensity (UACI) are used with below formula:

$$NPCR = \frac{100\%}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\right) \quad (7)$$

$$UACI = \frac{100\%}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|P_1(i,j) - P_2(i,j)|}{L-1}\right) \quad (8)$$

A bipolar array D(i,j) is defined by

$$D(i,j) = \begin{cases} 0 & \text{if } P_1(i,j) = P_2(i,j) \\ 1 & \text{if } P_1(i,j) \neq P_2(i,j) \end{cases} \quad (9)$$

where P_1 and P_2 are the cipher-image before and after one pixel changed in a plain-image.

TABLE III. PLAINTEXT SENSITIVITY (NPCR, UACI)

Image	***Single form of proposed structure***		***Triple form of proposed structure***	
	NPCR	**UACI**	**NPCR**	**UACI**
Lenna	100	33.29	100	33.29
Baboon	100	33.39	100	33.43
Pepper	100	33.36	100	33.25

- Peak Signal-to-Noise Ratio (PSNR): It is the ratio of mean square difference between two images. To get the PSNR evaluation, it is necessary to calculate Mean Square Error (MSE).

$$MSE = \frac{1}{MN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N} (C(i,j) - H(i,j))^2\right) \quad (10)$$

C(i,j) and H(i,j) are the cover image and hidden image. And the formula of PSNR is defined as below:

$$PSNR = 10\log_{10}\left(\frac{L^2}{MSE}\right) \quad (11)$$

- Information Entropy (H(s)): The mathematic theory of data communication used to against entropy analysis and the best value is reaching to 8 [7]. The formula is shown as below:

$$H(s) = \sum_{i=1}^{2^M - 1} P(S_i)\log_2 \frac{1}{P(S_i)} \quad (12)$$

Where M is the number of pixel of cipher-image

TABLE IV. PEAK SIGNAL-TO-NOISE RATIO(PSNR) INFORMATION ENTROPY (H(S))

Image	*Single form of proposed structure*		*Triple form of proposed structure*	
	PSNR(db)	**H(s)**	**PSNR(db)**	**H(s)**
Lenna	6.6965	7.9980	6.6929	7.9979
Baboon	9.5602	7.9977	9.5612	7.9979
Pepper	8.2413	7.9977	8.2567	7.9977

- Correlation Coefficient: The value to find the correlation between plain-image and cipher-image. Good cryptography gives the low correlation.

TABLE V. CORRELATION COEFFICIENT (HORIZONTAL)

Image	**Horizontal**	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	-0.0027	0.0012
Baboon	-0.0018	-0.0017
Pepper	-4.3955×10^{-4}	5.2933×10^{-4}

TABLE VI. CORRELATION COEFFICIENT (VERTICAL)

Image	**Vertical**	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	-0.0022	0.0017
Baboon	8.5431×10^{-5}	4.1482×10^{-4}
Pepper	-7.8337×10^{-5}	-4.9636×10^{-4}

TABLE VII. CORRELATION COEFFICIENT (DIAGONAL)

Image	**Diagonal**	
	Single form of proposed structure	***Triple form of proposed structure***
Lenna	0.0030	1.0201×10^{-4}
Baboon	0.0014	0.0029
Pepper	-0.0015	-0.0055

B. Comparison and Discussion

The proposed structure, both provided with high security confirmation, while DES consists with weak key conduction and 3DES is made to ensure with the key but the performance is slow because of three times compare to DES [8]. However the length of the key can solve the problem from some attack, it still faces with meet-in-the-middle attack. The security comparison is shown as below [9]:

TABLE VIII. COMPARISON OF SECURITY CONFORMATION

Parameters	***Proposed structure (average)***	***Data Encryption Standard (average)***
PNCR	100	99.6643
PSNR(db)	8.166	7.6057
UACI	33.34	51.2491

But in terms of the complexity of both DES and 3-DES generally is made as O(m) that consist of 8 S-Box and many round of XOR Operation (16, 48) which is the main issue effects to the performance of the system. For the proposed structure, it works only with second order of convolution summation that can produce high performance conduction.

V. CONCLUSION

In this paper, we have presented the comparison results between the proposed structures of chaotic cryptography in digital filter with DES and Triple DES. Having computed the experiment, the security confirmation of each technique provided the similar exclamation while produced different performance of complexity running. A single form of chaotic cryptography in digital filter can obtain the best outstanding consideration among others.

ACKNOWLEDGMENT

The author would like to express gratefully attitude to AUN/Seed-net and thankful to International College of King Mongkut's Institute of Technology Ladkrabang for supporting the fund and material supply during my research process.

REFERENCES

[1] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.

[2] M-S. Liu, Y. Zhang, J. li, "Research on Improving Security of DES by Chaotic Mapping" IEEE, Proceedings of the 8th International Conference on Machine Learning and Cybernetics, Baoding, pp. 12-15, Jul 2009. K. Elissa, "Title of paper if known," unpublished.

[3] B.J. Saha, Arun, K.K. Kabi and C. "A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color Images" 2014 international Conference on Circuit, Power and Computing Technologies [ICCPCT].

[4] L. O. Chua and T. Lin, "Chaos in digital filters," IEEE Trans. Circuits Systs., vol. 35, no. 6, pp. 648-658, June 1988.

[5] M. George and A. Ioannis, "Cryptography with Chaos", Proceeding 5th Chaotic Modeling and simulation International Conference, June 2012.

[6] P. Reatrey, C. Sorawat and P. Jaruwit, "A New Key Generator for Data Encryption Using Chaos in Digital Filter", 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC 2017), 4-5 August 2017, Shah Aam, Malaysia

[7] C. Shannon, "Communication theory of secrecy system", Bell system Technical Journal 28:656-715, 1949.

[8] M. Ebrahim, S. Khan and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975-8887) Volume 61-No. 20, January 2013

[9] S. Soni, H. Agrawal and M. Sharma, " Analysis and Comparison between AES and DES Cryptographic Algorithm", IJEIT 2017