ASM Sc. J., 13, 2020
https://doi.org/10.32802/asmscj.2020.sm26(4.29)

Use of the CFEA Lossless Data Compression Method in Transmitting Encrypted Modified Baptista Symmetric Chaotic Cryptosystem Data

Muhamad Azlan Daud[1], Zahari Mahad[2], Mohamad Rafley Abdul Rasit[3] and Muhammad Asyraf Asbullah[4]

[1,3]*Preparatory Centre for Science and Technology, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia*

[2,4]*Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia,43400 UPM Serdang, Selangor, Malaysia*

To confirm applicability of a modified Baptista symmetric cryptosystem that is based on the chaotic dynamical system, the CFEA compression algorithm was used. Various ciphers that respond to the similar message input produced using Baptista symmetric cryptosystem. This modified Baptista type cryptosystem which is differ to the current practice of a symmetric cryptosystem is affected by the extension number of ciphertext. The CFEA compression algorithm is a lossless data compression algorithm. Although the domain used is greater than its defined range, yet the compression algorithm is supposed to have no problem of mapping elements. Our idea is to integrate the CFEA compression algorithm during data transmission, as a result, the number of ciphertexts was reduced from n ciphertext, where n∈Z^+ and n≥1, to only 2 ciphertexts. Instead of transmitting n ciphertext, only 2 ciphertexts were transmitted. Therefore, the purposed integrated algorithm has reduced the number of ciphertexts to be transmitted.

Keywords: Baptista; CFEA-algorithm; number of ciphertext; lossless; transmission

I. INTRODUCTION

The Baptista type cryptosystem experiences many cipher texts which against the customary technique of symmetric cryptosystem (Baptista, 1998). Be that as it may, its polyalphabetic figure structure draws the continuation of examination into empowering this application.

Compression plays an essential part in our daily routine and in real-world applications, as it purposely decreases the redundant usage of valuable resources. For examples such as memory space and the computational time for data to move around over network. In addition, compression also can effectively reduce the amount of communication by viably utilizing accessible transfer speed (bandwidth). To be specific, there are two kinds of compression, i.e. lossy and lossless.

Firstly, we will explain the lossy data compression technique, which works as follows. The first step is the decompression procedure of compressed information produces results with lost some data. The above-said technique is also known as irreversible compression, mainly because of the reconstruction of the exact original message is not possible during the decompression process. As lossy unable to generate exactly the 100% of the original message, thus differences between the message before and after decompressing process are unacceptable.

The focal point of this paper is on one “lossless data compression technique”. The technique compresses data information successfully without detail lost. Therefore, the intended information can be impeccably recreated. Certainly, after decompression, the said information remains in its original structure before compression. It is

*Corresponding author’s e-mail: azlan.daud@ums.edu.my

also known as reversible compression as the original data is reconstructed by the decompression process. An example is the ZIP file mechanism. Notably, the original data becomes smaller, hence through the current public bandwidth capacity, it is easier to be transmitted.

The number of the original text n, was reduced to two new text m_1 and m_2 (Mandangan *et. al.,* 2015) by CFEA-Technique. The technique used was a one to one function and also known as a lossless data compression technique.

Preceding transmission, this study used a novel lossless data compression strategy on the cipher text. This procedure has encouraged a conceivable functional deployment of the Baptista cryptosystem.

II. The Modified Baptista Cryptosystem and CFEA Technique

The Baptista variant cryptosystem (Ward, 2005) turned out to be secure against attacks like the one-time pad attack that occurred in the year 2003 (Alvarez et al., 2000). Consequently, the desirable attributes from the first Baptista cryptosystem were retained. This section dedicated to the complete version of the Baptista cryptosystem by means of matrix secret key based on IFS (Ward, 2005).

We remark that, the IFS involve of the following maps;

$$V_j(a,b) = \begin{pmatrix} p_j & q_j \\ r_j & s_j \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c_j \\ d_j \end{pmatrix}, j = 1,2,\dots,K \quad (1)$$

for $j = 1$. That is,

$$V_1 = \begin{pmatrix} a_{j+1} \\ b_{j+1} \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a_j \\ b_j \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix},$$

and let the matrix

$$X = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

consist of only elements within set $\{0, 1\}$.

Then, the 2×1 matrix

$$Y = \begin{pmatrix} a_j \\ b_j \end{pmatrix}$$

Contain values of Baptista ciphertext. While the matrix

$$Z = \begin{pmatrix} c \\ d \end{pmatrix}$$

be equal to zero (i.e. $Z = 0$).

A. Encryption Algorithm

A chaotic map was prepared.

i. A look-up table be composed of i ε -intervals were constructed.
ii. Each site was represented with $S_1, S_2, S_3, \dots, S_{i-1}, S_i$.
iii. The lower and the upper bound of the first interval is 0, and 1, respectively.
iv. A one-dimensional chaotic map was chosen. The logistic map;

$$y_{n+1} = by_n(1 - y_n) \text{ for } = 4 .$$

The matrix secret key was prepared.

i. A $t \times t$ matrix $([X]_{t\times t})$ such that its inverse $([X]_{t\times t}^{-1})$ exists was generated.

$$X = \begin{pmatrix} m_{11} & m_{12} & \dots & \dots & m_{1t} \\ m_{21} & \dots & \dots & \dots & m_{2t} \\ \vdots & \dots & & \dots & \vdots \\ \vdots & \dots & & \dots & \vdots \\ m_{t1} & m_{t2} & \dots & \dots & m_{tt} \end{pmatrix},$$

The elements of the matrix only incorporated from the set {0,1}. Now, such a matrix will be assigned as the secret key.

At this stage, a distorted plaintext was assembled such that;

i. Each plaintext was encrypted using Baptista method.
ii. LetC_1denoted as the iteration numbers.
iii. Suppose we have matrix of dimension$t \times 1$. Thus, each element of C_1 was grouped into this matrix. Subsequently, we use the following matrix multiplication:

$$[C_2]_{t\times 1} = [A]_{t\times t} \times [C_1]_{t\times 1},$$

B. CFEA-Technique

In recent years, there has been an increasing amount of work related to the application of the mathematical object namely the continued fraction, particularly for cryptanalysis, for instance (Asbullah & Ariffin, 2019) and (Asbullah *et. al.,* 2016). However, in this work, we use another technique which is a combination of the Continued Fraction and Euclidean Algorithm and called as the CFEA-Technique. The algorithm of CFEA-technique was proposed by (Hung & Mandangan, 2013; Mandangan *et. al.,* 2015), and presented as follows.

i. Compression procedure

Step 1: Let the set of original ciphertext as

$[C_2]_{1\times 1}, [C_2]_{2\times 1}, [C_2]_{3\times 1} \dots [C_2]_{(t-1)\times 1}, [C_2]_{t\times 1}$

Step 2: Using Continued Fraction method, the new ciphertext C_1^* and C_2^* was computed as follows

$$[C_2]_{1\times1}+\cfrac{1}{[C_2]_{2\times1}+\cfrac{1}{\vdots+\cfrac{1}{[C_2]_{(t-1)\times1}+\cfrac{1}{[C_2]_{t\times1}}}}}=\frac{C_1^*}{C_2^*}$$

C_1^* and C_2^* are the corresponding ciphertext, which being transmitted to the recipient.

ii. Decompression procedure

Using Euclidean algorithm, the following was computed,

$$C_1^* = C_2^* q_1 + r_1$$
$$q_1 = r_1 q_2 + r_2$$
$$q_2 = r_2 q_3 + r_3$$
$$\vdots$$
$$q_{n-2} = r_{n-2} q_{n-1} + r_{n-1}$$
$$q_{n-1} = r_{n-1} q_n + r_n$$

the algorithm was terminated when $r_n = 0$ where C_1^* and C_2^* were the compressed ciphertext, q_n is quotient and r_n is remainder for $n = 1, 2, 3, \dots, t$. Then

$$q_1, q_2, \dots, q_{n-1}, q_n$$
$$= [C_2]_{1\times1}, [C_2]_{2\times1}, \dots [C_2]_{(t-1)\times1}, [C_2]_{t\times1}$$

which was the set of original ciphertext.

C. *Decryption Algorithm*

Multiply $[X]_{t\times t}^{-1}$ with the following ciphertexts ($[C_2]_{t\times1}$).

i. The following matrix multiplication was used:

$$[C_1]_{t\times1} = [X]_{t\times t}^{-1} \times [C_2]_{t\times1},$$

ii. List of integers was resulted.

Each integer was used to iterate the logistic map. The logistic maps were iterated until it fell in the corresponding phase space of the first character and iterating was continued until the final character developed the original plaintext.

III. RESULTS AND DISCUSSIONS

The implementation compression CFEA-technique on Baptista cryptosystem is shown in the Figure 1.

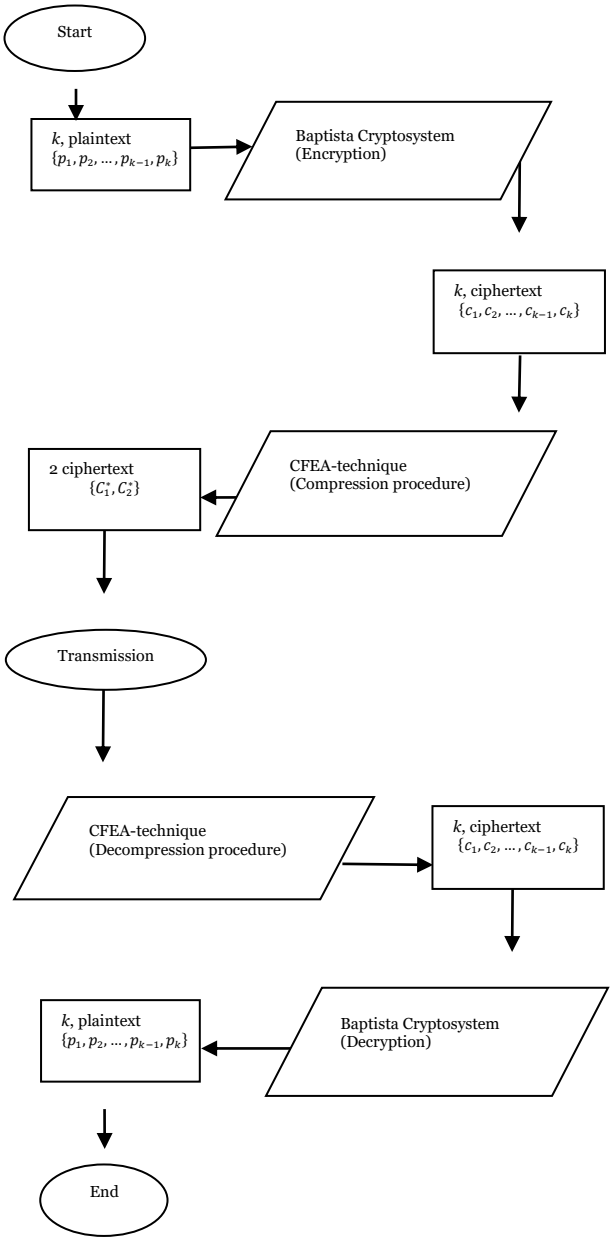

Figure 1: Implementation of CFEA-technique on Baptista cryptosystem

A. *Example 1*

Suppose S be the 26-alphabets source such that$S = \{A, B, C, \dots, Y, Z\}$ was used. The key X_0=0.232323 and parameter $b = 4$ were used as illustrative procedure. Let $P = ATTACKATDAWN$ be the text message.

1. *Encryption*

i. Choose $t = 2$.

ii. Matrix key was prepared, let

$$X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

iii. The encryption algorithm was applied from B.i.

iv. The following Plaintexts was used:

Table 1: Ciphertext after Baptista

Plaintext, *P*	**A**	**T**	**T**	**A**	**C**	**K**	**A**	**T**	**D**	**A**	**W**	**N**
Ciphertext, C_1	**8**	**63**	**25**	**19**	**1**	**1**	**55**	**4**	**33**	**3**	**4**	**134**

v. Next, for every integer C_1 was grouped into matrix with dimension $t \times 1$. From here the matrix multiplication was used as follows:

$$[C_2]_{t\times 1} = [X]_{t\times t} \times [C_1]_{t\times 1},$$

vi. The following Ciphertexts, C_2: 71, 63, 44, 19, 2, 1, 59, 4, 36, 3, 138, 134.

vii. The compression algorithm from B.ii was applied.

$$71 + \cfrac{1}{63 + \cfrac{1}{44 + \cfrac{1}{19 + \cfrac{1}{2 + \cfrac{1}{59 + \cfrac{1}{4 + \cfrac{1}{36 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{134}}}}}}}}}} = \frac{174845672599505}{2462064877201}$$

By using the CFEA-technique, these 12 ciphertexts was compressed to 2 ciphertexts. No matter how big the value of ciphertext, the number of ciphertexts will be reduced to 2 ciphertexts. Table 2 shows the number of ciphertexts transmitted.

Table 2: Comparison the number of ciphertext transmitted

Ciphertext	Number of Ciphertext transmitted without compression	Number of Ciphertext Transmitted With compression
71	12	2
63		
44		
19		
2		
1		
59		
4		
36		
3		
4		
134		

2. Decryption

i. By using decompression procedure of the CFEA-technique, the original 12-ciphertext recovered as follows.

$$174845672599505 = 2462064877201(71) + 39066318234$$
$$2462064877201 = 39066318234(63) + 886828459$$
$$39066318234 = 886828459(44) + 45866038$$
$$886828459 = 45866038(19) + 15373737$$
$$45866038 = 15373737(2) + 15118564$$
$$15373737 = 15118564(1) + 255173$$
$$15118564 = 255173(59) + 63357$$
$$255173 = 63357(4) + 1745$$
$$63357 = 1745(36) + 537$$
$$1745 = 537(3) + 134$$
$$537 = 134(4) + 1$$
$$134 = 1(134) + 0$$

ii. The algorithm terminated when $r = 0$. Then

Table 3: Comparison Quotient, q_i with Ciphertext, c_i

Quotient, q_i	Ciphertext, c_i
q_1	71
q_2	63
q_3	44
q_4	19
q_5	59
q_6	2
q_7	1
q_8	4
q_9	36
q_{10}	3
q_{11}	138
q_{12}	134

iii. Which is the set of original ciphertext,C_2: 71, 63, 44, 19, 2, 1, 59, 4, 36, 3, 138, 134.

iv. Algorithm B.3 used to decrypt the ciphertext, C_2 to obtain the original plaintext, $P = ATTACKATDAWN$.

From the result, the 12 ciphertext can be compressed to 2 ciphertext and will be sent to the receiver.

IV. CONCLUSION

This paper studied on CFEA-technique compression upon the Baptista cryptosystem. The result proved that CFEA-technique compression is applicable to Baptista cryptosystem.

Through this work, the k ciphertext can be compressed to 2 ciphertexts and will be sent to the receiver. Evidently, we show that our proposed algorithm could facilitate the Baptista cryptosystem towards a practical deployment.

As a continuation for possible future research, we are now working on finding a way to facilitate another algorithm which will enhance our result in this paper; i.e. to obtain a fast and efficient compression technique with reasonable ratio and speed for the deployment of the Baptista cryptosystem.

V. ACKNOWLEDGEMENT

The present research was fully supported under the grant UMS-SLB0156-2017.

VI. REFERENCES

Alvarez, Montoya, G., Romera, F. M. and Pastor. 2000, Cryptanalysis of a chaotic encryption system from Phys. Lett. A 276: 191-196.

Asbullah, M.A. and Ariffin, M.R.K. 2019, Another Proof of Wiener's Short Secret Exponent, Malaysian Journal of Sciences (MJS), (1), 62-68.

Asbullah, M.A., Ariffin, M.R.K. and Mahad, Z. 2016, Analysis on the Rabin-*p* cryptosystem. In *AIP Conference Proceedings,* Vol. 1787, No. 1, p. 080012.

Baptista, M.S. 1998, Cryptography with chaos from Phys. Lett. A 240: 50-54.

Hung, C. E. and Mandangan, A. 2013, Compression-RSA: New Approach of Encryption and Decryption Method, http://dx.doi.org/10.1063/1.4801103, American Institute of Physics.

Mandangan, A., Mei, L. C., Hung, C. E. and Hussin, C. H. C. 2015, CFEA-Technique: Smaller Size of the Compressed Plaintext. International Journal of Cryptology Research 5(1): 1-10.

Ward M.D. 2005, Exploring Data Compression via Binary Trees, 143-150.