International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2020.3601

E-ISSN : 2454-6135

Volume.6, Issue 2
February -2020

Chaos-Modified Lightweight Present Algorithm for Image Encryption

Ahmed Abd Ali Abd Ulkadhim[1]

[1] Computer Science Department,Faculty of Education,

Mustansiriya University,Baghdad ,Iraq

ABSTRACT

At the present time, the increase of data transmission over various networks in a wide range, which led to the need for a high level of security. One of the most important methods that have been invented to protect and integrity data is encryption. This paper test the efficiency of an algorithm for image encryption that utilizes a Lightweight present algorithm whit a chaotic logistic map equation. Where we relied on the chaos to produce the keys that were used in the proposed algorithm. Through the results, we observed that the modified algorithm is faster and safer. Also, the correlation neighboring pixels is about 0; no relationship at all between the two image versions. , the proposed algorithm gets better the encryption efficiency compared The original algorithm

Key Words: *Chaos, Present Algorithm, Image Encryption.*

1. INTRODUCTION

Image encryption has proven to be a successful way of communicating confidential information with countless procedures discovered. However, it continues to attract researchers as the use of images in all means of digital communication has increased significantly. Hence there is a tremendous growth in the use of computers, networks, communications and multimedia applications. The security of multimedia data is very important for online multimedia trading such as video on demand and real time video multicast. Image encryption is widely used to secure data transmission in open internet business. Each data has unique features so different data requires a different kind of encryption algorithm [1]. Many of the available algorithms are suitable for text data but not suitable for multimedia data such as photos and videos. Moreover, the traditional encryption algorithms available for data security are often not fast enough to handle as little memory as mobile devices. Due to the increasing demand for information security, image coding has become an important research field with broad application prospects. Image security is a major concern as web attacks become more dangerous[2].

In 2013 Sufyan and etal suggested a way to improve PRESENT Lightweight Algorithm, Where they worked on by selected one S-box out of 16 good S-boxes. Introductory analysis of linear and differential cryptanalysis is showing that the suggest algorithm is extra secure than stable PRESENT S-box [3].

.

In 2019 Srikanth Parikibandla, Sreenivas Alluri proposed, a Lorentz-based PRESENT architecture (LCS) has been introduced that considers key size as significant encryption challenges and this is a new way to overcome this issue and improve security[4].

Since the chaos system is sensitive to We proposed a new and effective method of generating keys via the chaotic system. its initial value It generates unpredictable values, so these values are used as keys to the Present algorithm, and we notice .that the results obtained are better and faster

2. LOGISTIC MAP

Logistic map is an easy non-linear function but wide used by authors. It's known in equation.

$$X_{n+1} = rX_n(1 - X_n) \qquad (1)$$

The logistic map generates random numbers Sequential using two parameters, 0< r 4 and {xi} is a floating number in (0,1), i = 0, 1, 2, 3 ..,n. When r > 3.75 and where 0 < xi < 1. {X0} initial value used to generated a series element{x1, x2,.....,xn}

it is neither periodic nor convergent That was, it has chaotic behavior There is a graphical method that shows the phenomenon as shown in the figure 1,Information about system dynamics Bring it by the bifurcation map brings information about the dynamics of the system [5].

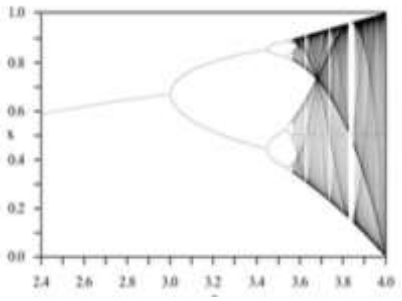

Figure.1 logistic map [6]

3. PRESENT ALGORITHM

The PRESENT block cipher, Illustrated in Figure 2, is an -lightweight substitution-permutation grid and depend of 31 tour. The block length is 64 bits. The cipher shore 80 and 128-bit secret keys. Each tour of PRESENT depend of three stages key addition, non-linear substitution layer, and bit wise [7].

3.1 Permutation layer Key addition As the first stage of ith tour, for1 ≤ i ≤ 32, the stream case is join using bit-wise XOR with the ith tour sub key.

$$Si\,j \rightarrow Si\,j \oplus Ki\,j, for\ 0 \leq j \leq 63\ and\ 1 \leq i \leq 32$$

$$where\ K32\ is\ used\ for\ post\ whitening.$$

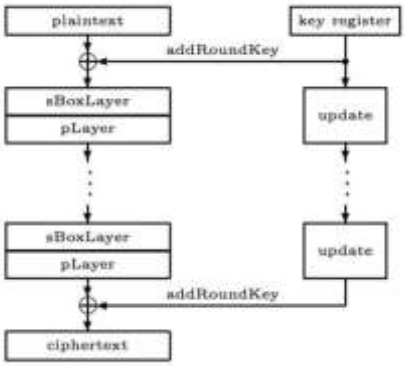

Figure .2 the present block cipher [8]

3.2 Substitution layer(S-box)

The produce of the key addition step goes through the S-box layer which is the non-linear process of the tour. The S-box applied in PRESENT is a solo 4-bit to 4-bit S-box which is utilized 16 times in parallel [9]

3.3 Permutation layer P

At the last stage of produce of s-box layer is rearranged to the permutation layer, After this process, bit i of the Present stage is Transferred to the bit position P(i). Two keys lengths are 80 and 128 bits supported by the key schedule algorithm [10]

4. THE PROPOSED METHOD

In this research, we proposed a new method for generating keys that is more suitable for the encryption algorithm. The blocks are lightweight in terms of performance, cost, and safety. To create the keys to an algorithm, we used the chaos system in our

DOI : 10.31695/IJERAT.2020.3601

proposed method. Initial value leads to hypersensitive pathways. Using a chaotic map, attackers cannot analyze information from encrypted images.

Where in the traditional method of al-algorithm, the key is generated by generating a primary value, and then these values are updated at the next stage to be the second key .In this case, the generation of serial keys may be subjected to breakage and analysis either. In our proposed method, it depends on the Logistic map of generating keys that cannot predicted or known as shown in following figure(3)

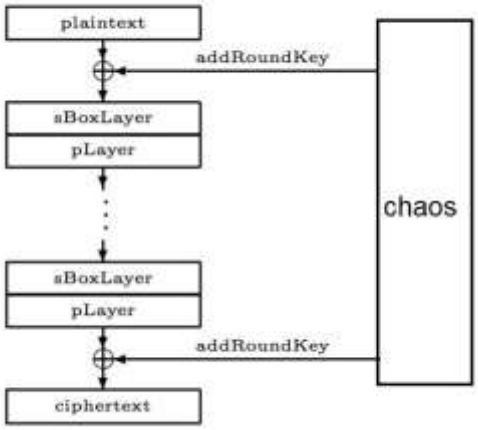

Figure.3 Modified present algorithm

4.1 The following steps for Modified present algorithm

Step1 Generate round key from chaos (Logistic map)

Step2 initial value and Parameters //for Logistic map

Step3 repeat step3 to N // where N=32

Step4 $Xn + 1 = rXn(1 - Xn)$

Step5 save the values generated from the chaos in Ki

Step6 For i=1 to 31 do //repeat round

Step7 add round key(STATE ,Ki) generated from chaos

Step8 SBox layer (STATE)

Step9 player

Step10 end for

add round key(STATE ,Ki)

5. THE RESULT

In this step, the efficiency of the proposed method is evaluated by time, image coefficients, and correlations. And later, compared to other methods that showed the results of this algorithm. Through the table, we note that Entropy is 7.884 as an average of five images close to the ideal value of 8.Table 1 shows the entropy of a different image through the result, note that the correlation between image pixels is less than the proposed algorithm, and this indicates that the proposed algorithm is better, and that the processing time is less compared to the traditional algorithm, as shown in Table 1

DOI : 10.31695/IJERAT.2020.3601

Table 1. The result for modify algorithm

Images	Present Algorithm			Modification Present Algorithm		
	Time	Correlation	Entropy	Time	Correlation	Entropy
Im1	103ms	0.0299	6.987	80ms	0.0123	7.801
Im2	90ms	0.0199	7.001	60ms	0.0188	7.906
Im3	87ms	0.0201	6.009	78ms	0.0194	7.899
Im4	107ms	0.0188	7.004	59ms	0.0104	7.901
Im5	98ms	0.0209	6.897	23ms	0.0097	7.913
total	97ms	0.0219	6.779	60ms	0.0141	7.884

The figure (4),(5) shows the time and correlation for the original and modified algorithm

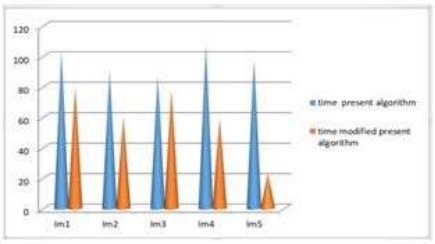

Figure .4 times for the original and modified algorithm

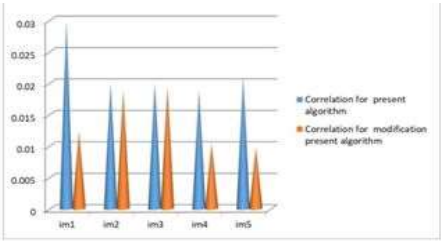

Figure .5 correlations for the original and modified algorithm

6. CONCLUSION

From The suggested way to modify the algorithm we note We note through the table that the velocity has increased from(97 ms to 60ms) as average for five images , also during the results of the table we note that the result is improved for Correlation and Entropy from (0.0219 to 0.0141 and 6.779 to 7.884).

REFERENCE

1 .Wang, Y., Wong, K. W., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. Applied soft computing, 11(1), 514-522

2. Wang, X., Teng, L., & Qin, X. (2012). A novel colour image encryption algorithm based on chaos. Signal Processing, 92(4), 1101-1108

3. AlDabbagh, S. S. M., & Al Shaikhli, I. F. T. (2013, December). Improving PRESENT lightweight algorithm. In 2013 International Conference on Advanced Computer Science Applications and Technologies (pp. 254-258). IEEE

4. Azzaz, M. S., Tanougast, C., Sadoudi, S., Fellah, R., & Dandache, A. (2013). A new auto-switched chaotic system and its FPGA implementation. Communications in Nonlinear Science and Numerical Simulation, 18(7), 1792-1804

5. Mankar, V. H., Das, T. S., & Sarkar, S. K. (2012). Discrete chaotic sequence based on logistic map in digital .communications. arXiv preprint arXiv:1207.2694

6. Wu, G. C., & Baleanu, D. (2014). Discrete fractional logistic map and its chaos. Nonlinear Dynamics, 75(1-2), 283-287

7. Bagheri, N., Ebrahimpour, R., & Ghaedi, N. (2013). New differential fault analysis on PRESENT. EURASIP Journal on Advances in Signal Processing, 2013(1), 145

8. Hoomod, H. K., & Ali, A. A. New Technique for Internet of Things Security based on the Hybrid Mcrypton-Blowfish and Chaotic System

DOI : 10.31695/IJERAT.2020.3601

9. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007, . September). PRESENT: An ultra-lightweight block cipher. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 450-466). Springer, Berlin, Heidelberg

10. Wang, M. (2008, June). Differential cryptanalysis of reduced-round PRESENT. In International Conference on Cryptology in Africa (pp. 40-49). Springer, Berlin, Heidelberg

.

DOI : 10.31695/IJERAT.2020.3601