International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2020.33759

Volume 6, Issue 3
March - 2020

Image Encryption Using Modification Blowfish Algorithm

Zynab M. jasim

Department of Computer Science/ Collage of Education

Mustansiriyah University

Baghdad- Iraq

ABSTRACT

At present, the need for information security has become a necessity. Chaos is widely used in the cryptographic system as a cryptographic keys generator. These keys are the most important component in the system because the security of the cryptographic system depends entirely on its quality. These values of chaos will be used as keys for blowfish instead of original keys in rounds. This modification algorithm with messy obtained, better and faster results, Where the average time, correlation and entropy to encryption five images respectively is 0.09, 7.9271and 0.10988.

Key Words: Image encryption, Blowfish algorithm, Chaos.

1. INTRODUCTION

According to the fast growth of the Internet and communications networks, the secrecy of digital images sent over public networks must be protected[1]. Image protection becomes an important issue according to wide applications of image such as; military, national-security agencies and diplomatic affairs. Encryption is a way to keep the confidentiality of images. In order to achieve better image security, many image encryption algorithms have been developed but no single encryption algorithm pleases all types of images. Cryptography which is simply the science of securing sensitive and trusted information as it is stored on media or transmitted over communication network paths. Cryptographic algorithm is categorized into two different types symmetric and asymmetric key cryptography in the symmetric cipher systems, the sender and receiver use identical key in the cipher operation (encryption and decryption) [2]. Symmetric key methods can be categorized into two sets; either block ciphers or stream ciphers, a block cipher is the one where a block of plaintext is converted into ciphertext block of same length. One example of symmetric block cipher is blowfish. In 1993, Bruce Schneier designed the Blowfish algorithm that has many benefits. It is considered fast, free alternative to existing encryption algorithms and it is also appropriate to implement on hardware in an efficient manner.

2. RELATED WORK

In 2018 Theda Flare and etal were proposed a modified Blowfish encryption that uses 128-bit block size and 128-bit key to comply with minimum requirements as an encryption standard. The modification kept the original structure for easy migration but used two S-boxes to save memory. A derivation was added to prevent symmetry the performance of the algorithm was evaluated using time, an avalanche.

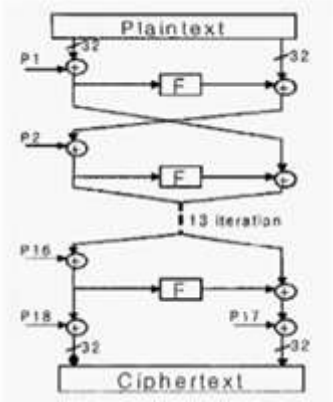
in 2018 Ariel Roy L. Reyes and etal, were suggested , a new modified version of the Blowfish encryption algorithm was introduced to support 128-bits block size input using the dynamic selection encryption method and reduction of cipher function execution through randomly determined rounds is introduced [4] .

In our suggested method, we will use these messy values as keys for the blowfish instead of the original keys for rounds. It was obtained from the modulation algorithm with better and faster messy results.

3. BLOWFISH ALGORITHM

Blowfish is a symmetric block cipher, the cipher is a 16-round Feistel network and uses password-dependent S-boxes. The power of the Blowfish algorithm depends on its sub-key generation and its basic confusion and diffusion based design [5]. Blowfish

encryption uses 18 each of 32- bit Permutation arrays precisely known as P-Boxes and 4 Substitution boxes referred as S-Box each of 32 bit size and having 256 entries each. It uses a Feaster cipher which is a general way of transforming a function into another function by using the concept of permutation, diffusion, confusion [6]. The working of blowfish cipher can be explained as follows, It separations the 64 bit block into two equal blocks having 32 bit size each, left block is XORed with first Sub array P1 and thus obtained result is fed in to a function called F-function. Inside the F-function substitution operations are carried out which in turn converts 32 bit blocks in to another 32 bit blocks. Thus resulted 32bit entries are XORed with the right half and the result obtained is exchanged as the left half for the next round. The feistal Structure of Blowfish Algorithm with 16 rounds of encryption is shown in the following Figures.1and 2 [7] .



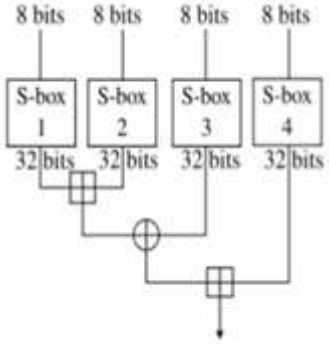


Figure1.blowfish algorithm **Figure2.s- boxes of blowfish**

3.1 The Hénon Chaotic map

Is two dimensional chaotic maps, It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. It takes a point (x_i, y_i) in the plane and maps it to a new point [8]

$$Xn+1 = 1+Yn - aXn\ 2 \quad \ldots\ldots\ldots\ldots \quad (1)$$
$$Yn+1 = bXn\ n=0, 1, 2\ldots$$

The map depends on two parameters, r and b, which for the canonical Hénon map have values of $r = 1.4$ and $b = 0.3$. For the canonical values the Hénon map is chaotic [9]

3.2 The proposed algorithm

By studying the blowfish algorithms and analyzing their work, which is encryption of the blowfish carries a risk, which is that the algorithm relies on the symmetric key, so if the key is discovered that will destroy the safety of the blowfish .Our method of modifying algorithm here depends on generating keys from the chaos system, and since the chaos system is sensitive to the initial value and produces random values that cannot be predicted. Where we use the values generated from the henon system and each generated value is used as a key that enters the round and the second round, we use another value as a second key for the second round and so on and up to the last round .Note the figure below that illustrates the modified algorithm.

DOI: 10.31695/IJASRE.2020.33759

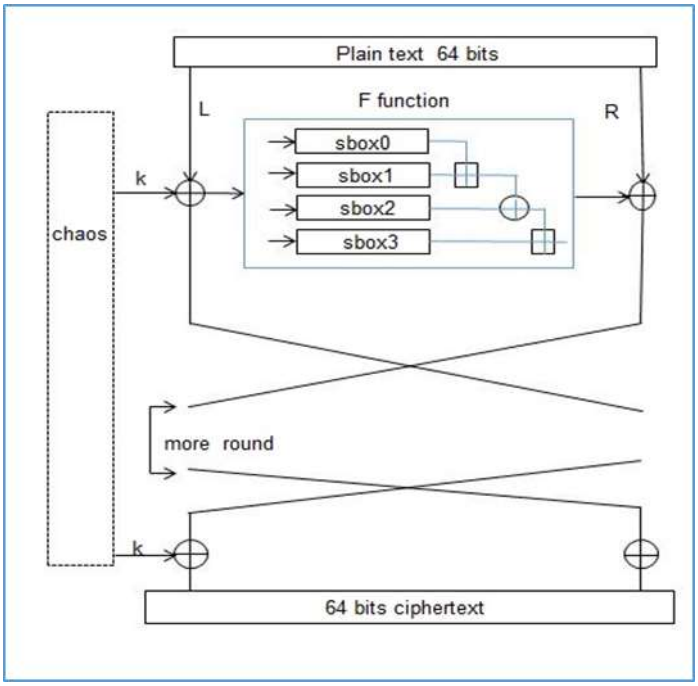


Figure3. Modified algorithm

3.3 Steps for the proposed modified algorithm

$step1$: $initial\ value\ and\ parameter\ (x(1) = 0, y(1) = 0, a = 1.4, b = 0.3)$
$Step2$:$for\ i$=2:N //$where\ n$=$number\ of\ key$
$step3$: (i) =1−1.4∗($x(i$−1)^2)+$y(i$−1)
$Step4$: (i) =b∗(i−1)
$Step5$: end
$Step6$: $Save\ the\ generated\ value\ from\ henon\ cha\ \ pi$
$Step7$: $Divide\ x\ into\ two\ 32-bit\ halves$: xL,
$step8$: $For\ i$ = 1to 16
$Step9$: $xL = XL\ XOR\ Pi$
$Step10$: $xR = (XL)\ XOR\ xR$
$Step11$:$Swap\ XL\ and\ xR$
$Step12$: $Swap\ XL\ and\ xR\ (Undo\ the\ last\ swap)$
$Step13$: $xR = xR\ XOR\ P17$
$Step14$: $xL = xL\ XOR\ P18$
$Step15$: $Recombine\ xL\ and\ xR$

4. RESULT AND DISCUSSION

The proposed system has been established using matlab programming language, Windows 7 with 64-bit operating system.We tested the system on five images, one size 128 * 128 pixels, to test the proposed system for encryption quality .Through the results, we have noticed that our proposed method is better and less likely to break .through the calculation of Correlation and entropy, as well as the proposed method was faster compared to the original algorithm As shown in the Figure4. , Figure5., and table (1).

DOI: 10.31695/IJASRE.2020.33759

Table (1) Time entropy and correlation for modification and original blowfish algorithm

images	blowfish algorithm			Modification blowfish algorithm		
	Time(ms)	Correlation	Entropy	Time(ms)	Correlation	Entropy
Im1	1.089	0.2889	7.4357	0.109	0.1895	7.8397
Im2	0.908	0.1948	7.6972	0.099	.00991	7.9902
Im3	2.001	0.4081	7.8856	0.089	0.1002	7.8899
Im4	1.905	0.3987	7.5029	1.001	0.1709	7.9001
Im5	0.872	0.5809	7.9171	0.091	0.0789	7.9271
average	1.355	0.37428	7.6877	0.2778	0.10988	7.9094

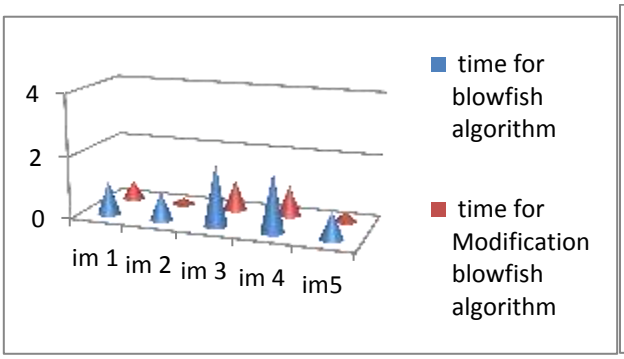


Figure4. Time

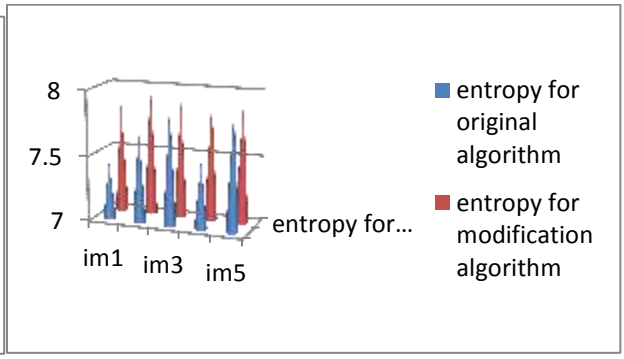
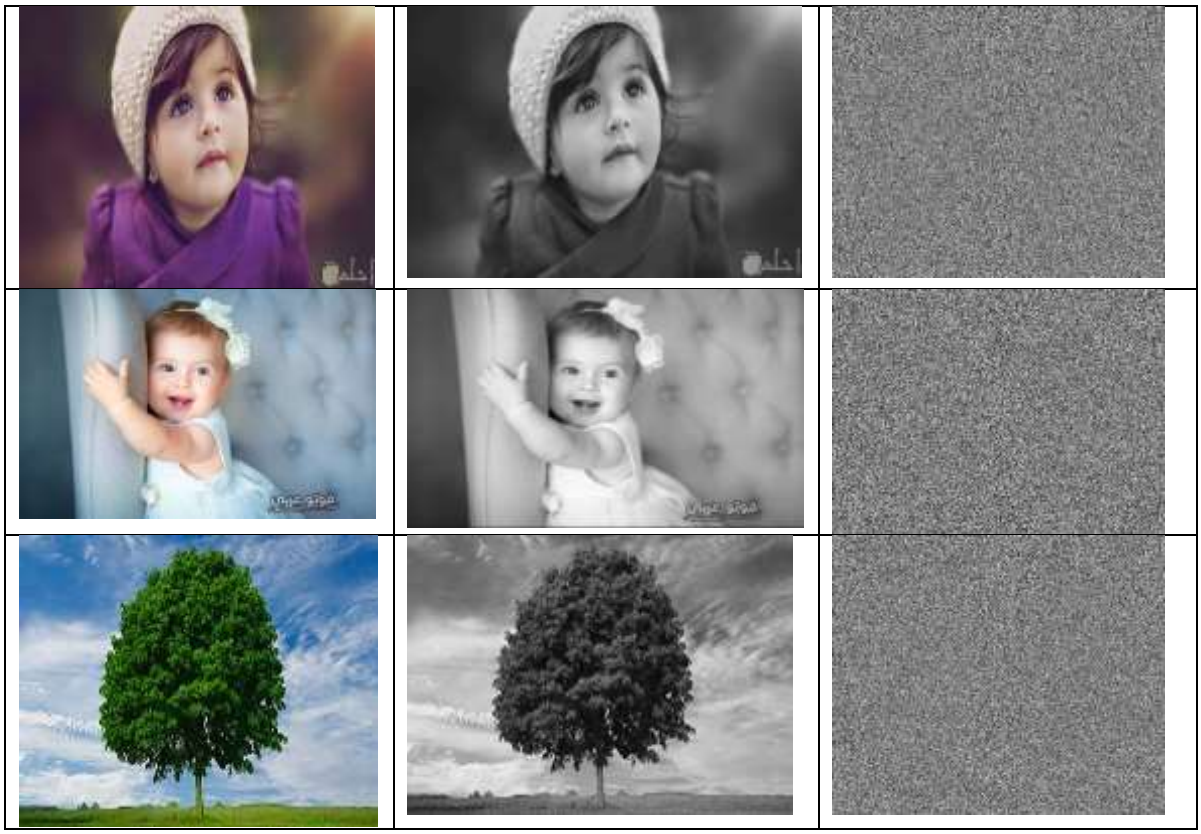


Figure5.Entropy



DOI: 10.31695/IJASRE.2020.33759

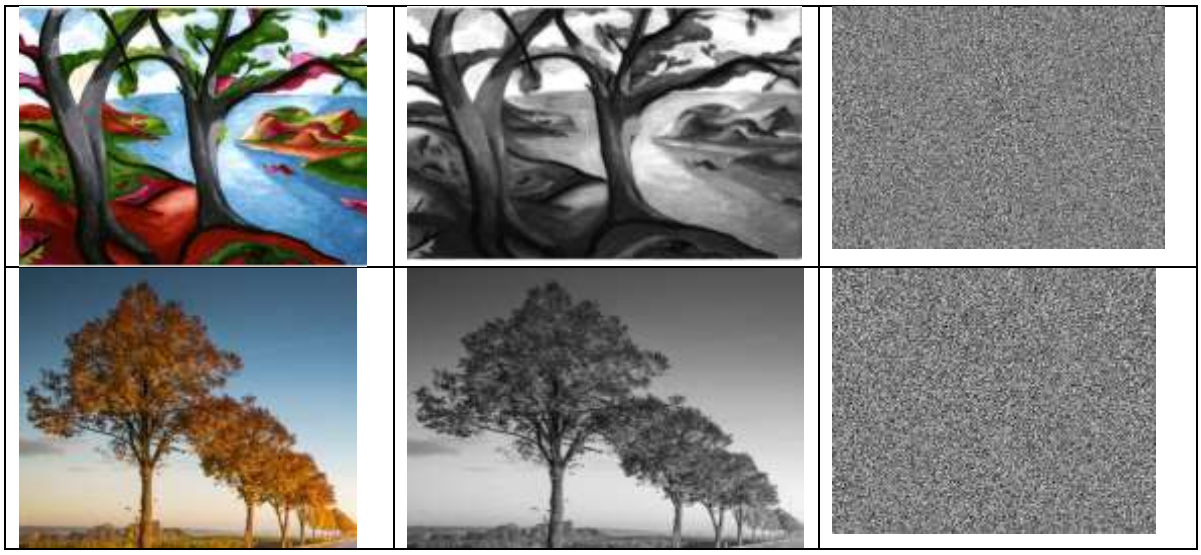


Figure6. Use the propose algorithm for images encryption

5. CONCLUSION

Dependent on modified In this paper we presented a new way for encryption algorithm with chaos, tested for image encryption, based on the results in the table where. The results of the security tests obtained show the robustness of the suggested algorithm against various attacks. This is due to the generation of keys from the chaotic system and is characterized by a high sensitivity to the secret key.

6. REFERENCES

1.Mandal, P. C. (2012). "Superiority of Blowfish algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, 29.

2. Singh,P.,& Singh, K. (2013). "Image encryption and decryption using blowfish algorithm in MATLAB", International Journal of Scientific & Engineering Research, 4(7), 150-154.

3. Quilala, T. F. G., Sison, A. M., & Medina, R. P. (2018). "Modified Blowfish Algorithm", Indonesian Journal of Electrical Engineering and Computer Science, 12(1), 38-45.

4. Reyes, A. R. L., Festijo, E. D., & Medina, R. P. (2018). Blowfish-128: "a modified blowfish algorithm that supports 128-bit block size", In 8th International Workshop on Computer Science and Engineering, Bangkok, Thailand (pp. 578-584.

5. Ashwaq T. Hashim, "Type-3 Feistel Network of The 128-bits Block Size Improved Blowfish Cryptographic Encryption", Received on: 28/5/2008 Accepted on: 6/11/2008.

6. Adam Young.,"Mitigating insider threats to RSA key generation". Crypto Bytes, 7(1):1–15, 2004.

7. Tahseen, I., & Habeeb, S. (2012). "Proposal new approach for blowfish algorithm by using random key generator", Journal of Madenat Alelem University College, 4(1), 5-13.

8. Wei-Bin, C., & Xin, Z. (2009, April). "Image encryption algorithm based on Henon chaotic system", In 2009 International Conference on Image Analysis and Signal Processing (pp. 94-97). IEEE.

9. Khan, J., Ahmad, J., & Hwang, S. O. (2015, May), "An efficient image encryption scheme based on: Henon map, skew tent map and S-Box", In 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO) (pp. 1-6). IEEE.

DOI: 10.31695/IJASRE.2020.33759