Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 4, November 2020, pp.2138-2145

A proposed lightweight image encryption using ChaCha with hyperchaotic maps

Mohammed Salih Mahdi[1], Raghad Abdulaali Azeez[2], Nidaa Falih Hassan[3]
[1] BIT, Business Information College, University of Information Technology and Communications, Baghdad, Iraq
[2] Collage of Education for Human Science-ibn rushed, University of Baghdad, Baghdad, Iraq
[3] Computer Science, University of Technology, Baghdad, Iraq

ABSTRACT

Image encryption plays a pivotal rule in enhancing telecommunications media. Since Privacy is necessary in our daily life in many areas, the personal image will be encrypted when it sent it over the Internet to the recipient to maintain privacy issue. In this paper, the image is encrypted using ChaCha symmetric stream cipher with Hyperchaotic Map. Due to the sensitivity characteristics of initial conditions, pseudo randomness chaotic maps and control parameters in chaotic, Hyperchaotic maps is use, higher security is obtained via using initial seed number, variance of parameters, and unpredictable direction of chaotic. The suggested lightweight image encryption has confirmed robustness contra brute force attacks by providing a massive key space. Furthermore, the suggested lightweight image encryption is eligible to defense from statistical cracking, insecurity of image based on criteria's histogram correlation and entropy.

Keywords: ChaCha, Hyperchaotic Map, Image Encryption, Lightweight, Stream Cipher

Corresponding Author:

Mohammed Salih Mahdi,
BIT, Business Information College,
University of Information Technology and Communications,
Baghdad, Iraq.
E-mail: mohammed.salih@uoitc.edu.iq

1. Introduction

In today's fast-moving and high-tech world, hiding of privacy and Information security become a significant role of everyone's [1-3]. Information security symbolizes an extremely base part in the communication era because it offers information defense services, chiefly at present-day times given the massive transfer of significant information over internet-media [4]. Cryptosystems have two classes, the first is, stream cipher and the second is, block cipher. The differences between the two categories are the processes of the converting the plain messages to cipher messages. The stream cipher algorithm makes the message encrypted as bit-by-bit with a mechanism of a secret key generator, and with the same algorithm, a decryption is done as the same encryption method, using the same secret key generator [5]. Many methods in the stream cipher can be used to generate the key for encrypt the messages like clock-controlled generators, non-linear combination generator, shift-register, etc. Contrast the stream cipher, is the block cipher which is done by convert a complete block in any time at once [6]. Various of stream algorithms such as salsa [7], Rabbit [8], HC128 [9] are used. Several block cipher algorithms such as RC5, DES [10] are used. Other classification is depending on how a secret key method is distributed, it classifies the crypto-systems into private-type (symmetric) key and public-type (asymmetric) key crypto-systems. In the private key, crypto-systems have the same key is used between the sender and receiver for encryption and decryption, respectively, on the other hand, in public key, when plaintext is encrypted by utilizing a public key, then it's ciphertext is decrypted using private key[11]. Different fields of studies like engineering, physics, economy, and biology used chaos theory in the past years, (nineties of the last century(, extensive studies done by many researches and scientists in the field of chaotic systems born from this theory. Researchers have reached the fact that there is a strong relation combine the two theories cryptography and chaos [12-14], but why chaotic theory are used closely with cryptography, to answer this question, there are three reasons, first, huge size of all multimedia which need real time operations, second highest correlations between pixels, block patterns, data redundancy, and frames of all

multimedia, third light weight encryption is one of the requirements of real time, due to the perceptual information preservation [15]. In encryption, application mathematical models to the chaotic systems like Henon map, Rossler, Lorenz and logistic map, attacks provide many attention [16]. Some of chaotic's characteristics that distinguished from other algorithms are: the initial states, control parameter, nonperiodicity of systems' trajectory for the states, randomization characteristics, and the nature of transitivity for the systems' behavior [17]. When chaotic stream cipher analyzed and demonstrated the problem of chaotic self_synchronization stream ciphers and open_loop_based chaotic synchronization stream ciphers which ciphertext is re-intered into encryption process. To avoid this problem, chosen-ciphertext-attack approach is used with self_synchronization 3_D chaotic stream cipher and decipher the algorithm with single key, then the ciphertext of it is fed back in to chaotic stream cipher, the encryption / decryption operations is done by low bits of state variable [18].Ying N., et al in [19] suggest a technique to encrypt the gray image using hyper chaos cipher, combine it with DNA sequence code to produce a confusion model, based on shifting the position of pixels, and spread them by using Chen Chaos method. DNA coding process is enhanced by repeating, propagating and confusing the characteristics with modify Quadruple hyperbolic sequence technique. Chenghai Li., et al in [20] presents ciphering scheme to encrypt color image. After convert the image to one dimensional gray image and the position of the pixels were changed according to the four-dimensional hyperchaotic system. From the plain text, the number of iterations was calculated and these iterations are representing as encryption keys to increase key space and the ability to baffle plaintext attack. Ammar M. R., et al in [21] present a cipher model for encrypt any multimedia such as text, voice, and video by using Henon and double chaotic maps Logistic. The random chaotic maps imply the two models which are speech scrambling and Simulink, they were more successful due to the highest sensitivity of the initial values and the external model of the parameters. Ibtisam A. et al in [22] design a cipher system for color image using diffusion, confusion and shuffled concept based on Chen hyper. Keys is supplied by hyperchaotic maps, which are sine chaotic map and the logistic map 1D, combined them, then, the cipher image is XORed with the keys to produce good encrypted image against brute force attack and various kind of threats. [23] suggest a method to encrypt gray image by used logistic map for get Pseudo-Random-Number-Generator (PRNG) to feed two sequences, first, is plaintext sequence (permuted with it), and the second is DNA sequence (for generate random DNA sequence), these sequences are XORed each with other to produce encrypted image.

From this point of view, the contribution of this research suggests lightweight image encryption according to ChaCha with hyperchaotic maps in telecommunications internet-media. ChaCha stream cipher is utilized as a modern and rapid symmetric lightweight cryptography, ideally utilized in the situation of procedures and apps according to one of the following causes is discover: 1. poor source for creating random key, 2. lower computing power with a force brute force attack. Hyperchaotic maps is utilized as the increasing complexity of the initial seed of hyperchaotic maps, the attacker missed the ability to listen to the cryptosystem method, even though he/ she realized the plain_image.

2. Preliminaries

2.1. ChaCha structure

In 2005, ChaCha is a stream cipher is utilized by Google comparable to salsa cipher. Three major processes on the ChaCha is done which are addition process, XOR process, and rotation process. In encryption, the initial state of ChaCha is stored with sixteen 32-bit word values shown in Table 1, the keywords are the copy of the input word that is block counter and nonce, in each round, add the keys to the constants, XOR the output to the inputs, rotate them, add the results to the keys and so on. [24-25]. In ChaCha, the diffusion quantity is expanding per round, this led to more secure iterations. [26-28]. ChaCha is a symmetric stream cipher used identical computation process, according to columns form followed by diagonals form as illustrated in Figure 1 and Figure 2 [29-31].

Table 1. Input state of ChaCha

Cons	Cons	Cons	Cons
Key	Key	Key	Key
Key	Key	Key	Key
Input	Input	Input	Input

Column form	Diagonal form
QR(x 0 , x 4 , x 8 , x 12)	QR(x 0 , x 5 , x 10 , x 15)
QR(x 1 , x 5 , x 9 , x 13)	QR(x 1 , x 6 , x 11 , x 12)
QR(x 2 , x 6 , x 10 , x 14)	QR(x 2 , x 7 , x 8 , x 13)
QR(x 3 , x 7 , x 11 , x 15)	QR(x 3 , x 4 , x 9 , x 14)

Figure 1. Quarter functions of ChaCha

$$a = a + b,\quad d = (d \oplus a) \ll 16$$
$$c = c + d,\quad b = (b \oplus c) \ll 12$$
$$a = a + b,\quad d = (d \oplus a) \ll 8$$
$$c = c + d,\quad b = (b \oplus c) \ll 7$$

Figure 2. Process functions of ChaCha

2.2. Hyperchaotic schema

From a technical point of view, hyperchaotic is a developed technique from chaos theory with more arbitrary behavior and unpredictability of values. Furthermore, it has a massive Key_space, higher complexity and it occurs as 4D non_linear form. Hyperchaotic is specified by [32]:

$$K_1 = a(K_2 - K_1) + b_1 K_4$$
$$K_2 = cK_1 - K_1K_3 + b_2K_4$$
$$K_3 = -dK_3 + K_1K_2 + b_3K_4$$
$$K_4 = -e\ K_1$$

Where initial parameters of hyperchaotic can be specified by Table 2:

Table 2. Initial parameters of hyperchaotic

Parameters	Values
a	35
b_1	1
b_2	0.2
b_3	0.3
c	35
d	3
e	5

3. Suggested methodology

The schema of the suggested methodology be made up of two essential points and explained in Figure 3. The first point of suggested methodology combines the robustness of hyperchaotic schema with ChaCha Structure to generated keys, the seed keys of ChaCha Structure are generated based on the hyperchaotic schema that serve as undisclosed seed key to increase the efficiency of generated keys as explained in Algorithm (1):
The second point of suggested methodology is to suggest lightweight image encryption according to split image into 8 regions explained in Figure 4 and implements the subsequent operations:

- $Operation_1$: Shuffling the eight regions of image according to key-secret map explained in Figure 5. Key-Secret map is vector of 8 positions with random values (from 1 to 8).
- $Operation_2$: Merge the output of eight regions images of $Operation_1$ to single image explained in Figure 6.
- $Operation_3$: Convert single image of $Operation_2$ to binary form.
- $Operation_4$: Scrambling binary pixels by utilizing XOR with the generated key of ChaCha which is generated by first phase explained in Figure 7.

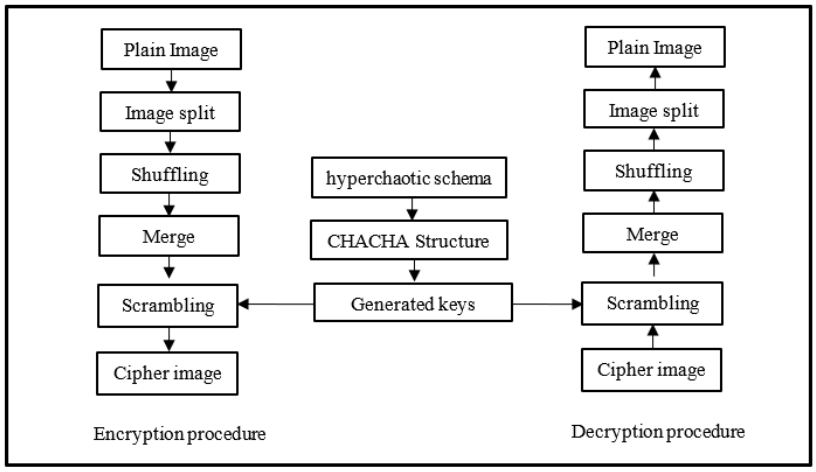


Figure 3. The Suggested Methodology

Algorithm (1): Suggested keystream Generator based on ChaCha and the hyperchaotic schema

Input: Iinitial parameters of hyperchaotic

Output: keystream

Begin

Step$_1$: Run the hyperchaotic schema 1000 rounds to minify the cross effects. **Step$_2$**: Run the hyperchaotic schema 4 rounds after step$_1$(From 1001 to 1004 round), 4 keys will be extracted for each round according to:

$$Z_1^r = (k_1^r * 10^{15}) \% 2^{32}\text{-}1$$

$$Z_2^r = (k_2^r * 10^{15}) \% 2^{32}\text{-}1$$

$$Z_3^r = (k_3^r * 10^{15}) \% 2^{32}\text{-}1$$

$$Z_4^r = (k_4^r * 10^{15}) \% 2^{32}\text{-}1$$

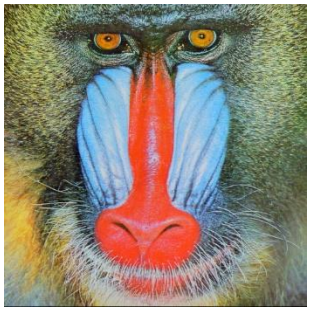
where r acts the round index.

Step$_3$: 16 values will be extracted from step$_2$ that is act the initial seed keys of ChaCha Structure (key, nonce, counter and constants).

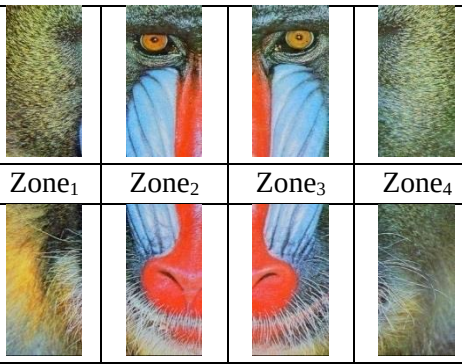
Step$_4$: ChaCha runs 20 rounds according to hyperchaotic-seed keys of step$_3$ to mix keys and generate unpredictability keys.

Step$_5$: Convert hyperchaotic-seed keys to binary keystream

End



a: Original Image (Baboon 256*256)



b: 8 Baboon regions

Figure 4. Sample of image split

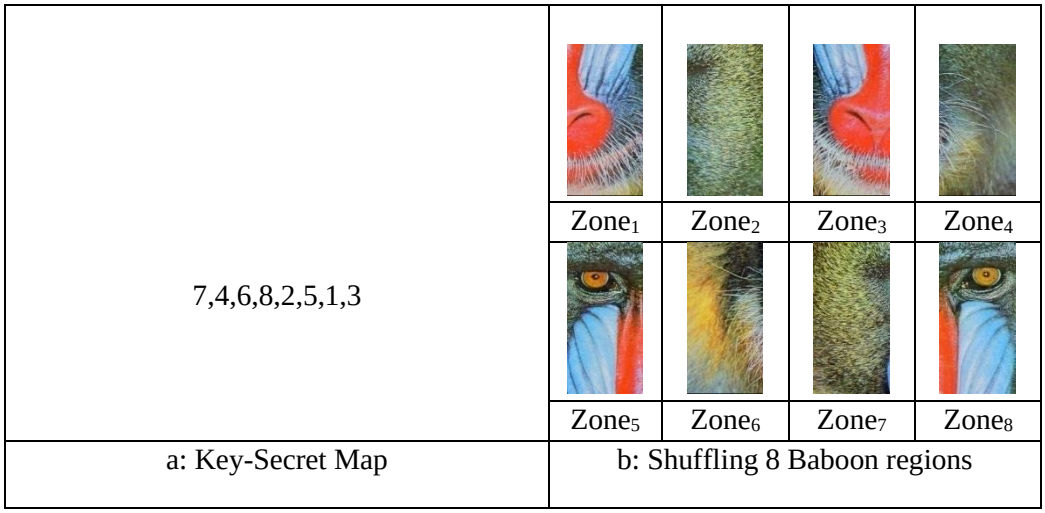


Figure 5. Sample of shuffling image split

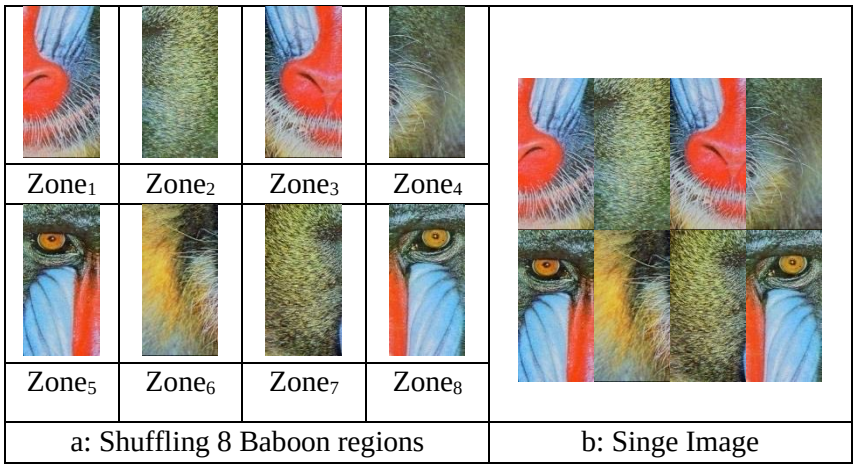


Figure 6. Sample of merge shuffling image regions

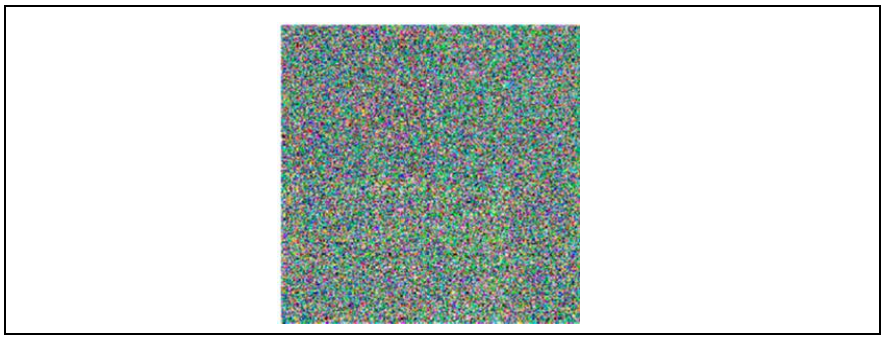


Figure 7. Sample of scrambling single image

4. Results

The schema of the suggested methodology was tested on standard images (256*256). The python 3.9 was utilized to run the suggested lightweight image encryption based on ChaCha with Hyperchaotic Maps. The initial parameters of hyperchaotic can be specified by Table 1 were utilized to offer a chaotic key as the initial seed keys of ChaCha Structure. Splitting, shuffling and scrambling operations were on original image to have encrypted image by utilizing XOR with the generated keys of ChaCha. Set of criteria is utilized for check the Security Analysis of the schema of the suggested methodology: -

- ***Key space:*** this factor of suggested lightweight image encryption based on ChaCha with hyperchaotic maps is comprised of initial conditions of K_1, k_2 with same ranges (-50 to 50), k_3 with ranges (1 to 92) and k_4 with ranges (-300 to 300) with step volume 10^{-13}, and require 8! for key-secret map. Furthermore, breaking ChaCha schema requires 2^{512} iteration. thus, the suggested lightweight image encryption is eligible to defense from brute-force cracking**.**
- ***Histogram:*** the histogram of the suggested lightweight image encryption based on ChaCha with hyperchaotic maps is an essential criterion to prove that the suggested lightweight image encryption is eligible to defense from statistical cracking explaining in Figure 8, by introducing stabilization and smoothing for histogram-encryption image and obvious peak and non-uniformity indictor for histogram-original image.

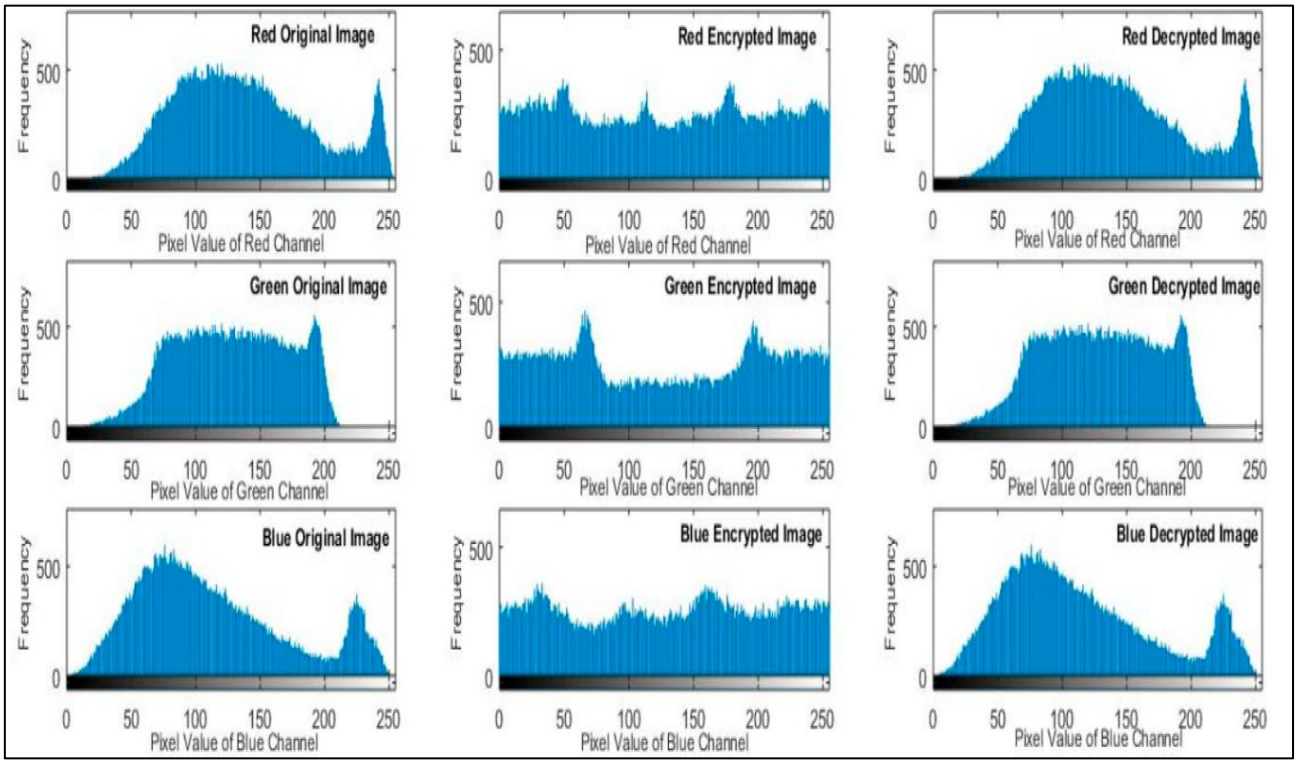


Figure 8. Sample of histograms of original image (Baboon 256*256), encrypted and decrypted image in RGB channel

- ***Entropy:*** the entropy of the suggested lightweight image encryption based on ChaCha with hyperchaotic maps is an essential feature to prove that the suggested lightweight image encryption is eligible to defense from insecurity of image explaining in Table 3 by providing entropy value which is near to critical value (eight).
-

Table 3. Sample of entropy of encrypted Image

Image	Red	Green	Blue
Baboon	7.9983	7.9991	7.9993

- ***Correlation:*** the correlation of the suggested lightweight image encryption based on ChaCha with hyperchaotic maps is confirming the robustness of suggested lightweight image encryption. Figure 9 depicts horizontally correlation the two_neighboring pixels of plain-image (near to critical value (1)) and encrypted image (near to critical value (0)).

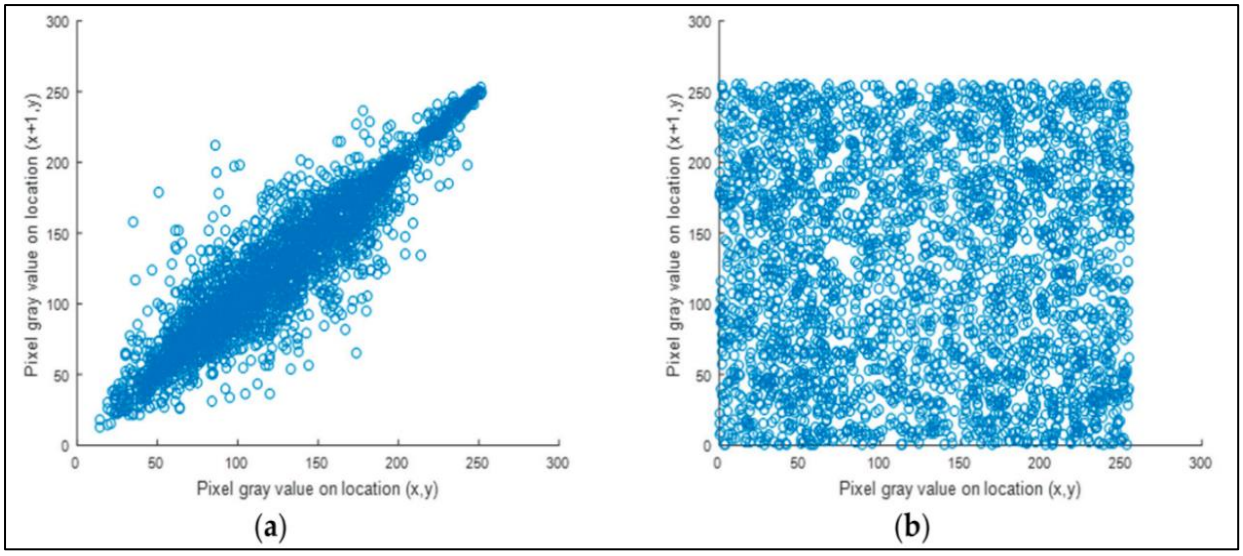


Figure 9. Sample of horizontal correlation of original image (Baboon 256*256) and encrypted image

5. Conclusions

Internet is used from all people because it is a public media tool for everyone to get information from any ware. Secret communication is an important issue in our live, utilizing the algorithms for encrypting secret image, it will not be perfect because image file needs a higher dynamic system. this paper has suggested lightweight image encryption based on ChaCha with hyperchaotic maps for the target of encrypting image in communications which is sending images on unprotected networks and smartphones. The depicted suggested lightweight image encryption has confirmed robustness contra brute force attacks by providing a massive key space. Furthermore, the suggested lightweight image encryption is eligible to defense from statistical cracking, insecurity of image based on criteria's histogram and entropy respectively, and correlation criteria of the suggested lightweight image encryption has discovered horizontally correlation the 2 neighboring pixels of plain-image (near to critical value (1)) and encrypted image (near to critical value (0)). The consuming time of the suggested lightweight image encryption require about 3.5 seconds that referred it can run on real_time programs.

References

[1] H. K. Tayyeh, M. S. Mahdi, and A. S. A. AL-Jumaili. "Novel steganography scheme using Arabic text features in Holy Quran." International Journal of Electrical & Computer Engineering (2088-8708) 9.3 (2019).

[2] M. S. Mahdi, and N. F. Hassan. "A Proposed Lossy Image Compression based on Multiplication Table." Kurdistan Journal of Applied Research 2.3 (2017): 98-102.

[3] M. S. Mahdi, and N. F. Hassan. "Design of keystream Generator utilizing Firefly Algorithm." Journal of Al-Qadisiyah for computer science and mathematics 10.3 (2018): Page-91.

[4] A. K. Farhan, and M. Salih. "Proposal of New Keys Generator for DES Algorithms Depending on Multi Techniques." Engineering and Technology Journal 32.1 Part (B) Scientific (2014): 94-106.

[5] D. D. Salman, R. A. Azeez, and A.-M. J. Abdul-Hossen. "BUILD CRYPTOGRAPHIC SYSTEM FROM MULTI-BIOMETRICS USING MEERKAT ALGORITHM," Iraqi J. Comput. Informatics ijci, vol. 45, no. 2, pp. 1–8, 2019.

[6] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A proposal for the advanced encryption standard," NIST AES Propos., vol. 174, pp. 1–23, 1998.

[7] M. S. Mahdi, and N. F. Hassan. "A SUGGESTED SUPER SALSA STREAM CIPHER." Iraqi Journal for Computers and Informatics ijci 44.2 (2018).

[8] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, "Rabbit: A new high-performance stream cipher," in International Workshop on Fast Software Encryption, 2003, pp. 307–329.

[9] S. Raizada, “Some results on analysis and implementation of HC-128 stream cipher.” Indian Statistical Institute, Kolkata, 2015.
[10] A. K. Farhan, M. S. Mahdi,"Proposal Dynamic Keys Generator for DES algorithms", islamic college university journal, 29 ,(2014): 25-48
[11] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, Computer security: principles and practice. Pearson Education Upper Saddle River, NJ, USA, 2012.
[12] T. Gao and Z. Chen, “Image encryption based on a new total shuffling algorithm,” Chaos, solitons & fractals, vol. 38, no. 1, pp. 213–220, 2008.
[13] H. Ansaf, H. Najm, J. M. Atiyah, O. A. Hassen, " Improved Approach for Identification of Real and Fake Smile using Chaos Theory and Principal Component Analysis ", Journal of Southwest Jiaotong University, Vol.54, No.5, 2019.
[14] H. Najm, H. K. Hoomod, R. Hassan, “Intelligent Internet of Everything (IOE) Data Collection for Health Care Monitor System “, International Journal of Advanced Science and Technology, Vol. 29, No. 4, 2020.
[15] Z. Su, G. Zhang, and J. Jiang, “Multimedia security: a survey of chaos-based encryption technology,” Mutimedia A Multidisiplinary Approach to Complex Issues, Ed. I. Karydis, InTech, pp. 99–124, 2012.
[16] A. A. Tamimi and A. M. Abdalla, “A double-shuffle image-encryption algorithm,” in Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV), 2012, p. 1.
[17] S. S. Askar, A. A. Karawia, and A. Alshamrani, “Image encryption algorithm based on chaotic economic model,” Math. Probl. Eng., vol. 2015, 2015.
[18] Z. Lin, G. Wang, X. Wang, S. Yu, and J. Lü, “Security performance analysis of a chaotic stream cipher,” Nonlinear Dyn., vol. 94, no. 2, pp. 1003–1017, 2018.
[19] Y. Niu, X. Zhang, and F. Han, “Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database,” Comput. Intell. Neurosci., vol. 2017, 2017.
[20] C. Li, F. Zhao, C. Liu, L. Lei, and J. Zhang, “A hyperchaotic color image encryption algorithm and security analysis,” Secur. Commun. Networks, vol. 2019, 2019.
[21] A. M. Raheema, S. B. Sadkhan, and S. M. A. Sattar, “Design and implementation of speech encryption based on hybrid chaotic maps,” in 2018 International Conference on Engineering Technology and their Applications (IICETA), 2018, pp. 112–117.
[22] I. A. Taqi and S. M. Hameed, “A new Color image Encryption based on multi Chaotic Maps,” Iraqi J. Sci., vol. 59, no. 4B, pp. 2117–2127, 2018.
[23] B. Mondal and T. Mandal, “A light weight secure image encryption scheme based on chaos & DNA computing,” J. King Saud Univ. Inf. Sci., vol. 29, no. 4, pp. 499–504, 2017.
[24] P. Yadav, I. Gupta, and S. K. Murthy, “Study and analysis of eSTREAM cipher Salsa and ChaCha,” in 2016 IEEE International Conference on Engineering and Technology (ICETECH), 2016, pp. 90–94.
[25] A. Czubak, A. Jasiński, and M. Szymanek, “A Note on Keys and Keystreams of ChaCha20 for Multi-key Channels,” in International Conference on Computer Networks, 2018, pp. 357–372.
[26] R. Velea, F. Gurzău, L. Mărgărit, I. Bica, and V.-V. Patriciu, “Performance of parallel ChaCha20 stream cipher,” in 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), 2016, pp. 391–396.
[27] D. J. Bernstein, “ChaCha, a variant of Salsa20,” in Workshop Record of SASC, 2008, vol. 8, pp. 3–5.
[28] Mohammed Salih Mahdi, and Nidaa Flaih Hassan, "Proposed an Efficient Secure Healthcare IoE ", University of Technology, PhD Thesis, Baghdad, Iraq, 2019.
[29] P. McLaren, W. J. Buchanan, G. Russell, and Z. Tan, “Deriving ChaCha20 key streams from targeted memory analysis,” J. Inf. Secur. Appl., vol. 48, p.102372, 2019.
[30] M. Almazrooie, A. Samsudin, and M. M. Singh, “Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map.,” JiPS, vol. 11, no. 2, p. 310, 2015.
[31] H. Najm, H. K. Hoomod, R. Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa20", Periodicals of Engineering and Natural Sciences,Vol 8, No 3, 2020
[32] C.-L . Li, S.-M. Yu. A new hyperchaotic system and its adaptive tracking control. Acta Physica Sinica -Chinese Edition, vol.61, no.4, 2012.