Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Developed Lightweight Cryptographic Algorithms for The Application of Image Encryption: A Review

Alaa Noori Mazher [a], *Jumana Waleed* [b] *and Abeer Tariq MaoLood* [c]

[a] *Department of Computer Science, University of Technology, Baghdad-Iraq, Email : 110027@uotechnology.edu.iq*

[b] *Department of Computer Science, College of Science, University of Diyala, Diyala -Iraq, Email: jumanawaleed@sciences.uodiyala.edu.iq*

[c] *Department of Computer Science, University of Technology, Baghdad-Iraq, Email: 110032@uotechnology.edu.iq*

ARTICLE INFO

Article history:
Received: 10 /04/2021
Rrevised form: 21 /04/2021
Accepted : 02/05/2021
Available online: 06/05/2021

Keywords:

Developed Lightweight Cryptographic Algorithms, Digital Image Encryption, Salsa20, ChaCha20.

ABSTRACT

As a consequence of the fast evolution of information technology, a substantial amount of digital information is created and disseminated over various kinds of networks. The digital image represents one of the most commonly utilized formats of digital data since it has a straight visual effect. Moreover, a digital image holds important possibilities and extra information, for instance, personal photographs are capable of conveying the persons' physical appearance as well as other details like their ages and health. So, it is significant to protect digital images from unauthorized accessing that certainly specifies the need for developing efficient lightweight cryptographic algorithms to ensure the digital images' privacy. In this review paper, several developed lightweight cryptographic algorithms and their application in digital image encryption were presented. Additionally, a comparative analysis of the recently existing related works was achieved for these developed algorithms.

MSC : 30C45 , 30C50

DOI : https://doi.org/10.29304/jqcm.2021.13.2.788

1. Introduction

In recent, multimedia takes an important portion in the entire individuals' digital communications. Consequently, the amount of transmitted and stored data of multimedia day-to-day has considerably increased [1]. Therefore, the assurance of data privacy and security represents a critical challenge for the experts of security [2]. Regrettably, traditional schemes of encryption such as DES, AES, and RSA are developed for textual data and these schemes are not

Corresponding author : *Jumana Waleed*

Email address: *jumanawaleed@sciences.uodiyala.edu.iq*

Communicated by: *Dr. Rana Jumaa Surayh aljanabi.*

appropriate for images' security since they have large size, strong correlation, and high redundancy [1]. There are lots of schemes that are available for securing digital images; these involve steganography [3], watermarking [4-8], encryption [9], and etc.

There are various schemes of image encryption have been proposed depending on various technologies and theories. Lightweight cryptography algorithms are a part of modern cryptographic algorithms that can be utilized within devices of low resources. These cryptographic algorithms do not specify hard criterion to classify cryptographic algorithms as lightweights, however, the prevalent attributes of any lightweight algorithm are extremely low needs for fundamental resources of base devices [10]. Recently, lightweight cryptography algorithms become relevant in the application of digital image encryption.

In order to solve the problem of creating effective algorithms of lightweight cryptography, there is a need for innovative approaches to modify the traditional algorithms with adaptation to the hardware attributes and systems' limitations at lower cost and find proper specialized solutions in algorithmic, methodological, software, and hardware terms.

This review paper is constructed as follows; The lightweight cryptographic algorithms and their types are briefly described in the next section, then the developed lightweight (Salsa20 and Chacha20) algorithms for image encryption application are presented in section three, after that, a performance comparison between these lightweight algorithms is explained in section four, finally, many conclusions are demonstrated in the last section.

2. Lightweight Cryptographic Algorithms

The implementation of cryptography has helped different information forms for being legally accessed via an authentic user with the assist of its typical processes of encryption. But, there are several differences when implementing encryption on ordinary files and on digital images [11]. The pixels' contents inside any digital image are infinite and so, the encryption algorithm relies on the sampling process as well. Recently, there are lots of developed researches that have concentrated on image encryption, however, until now there is no standard algorithm of encryption that provides full coverage of security standards (privacy, availability, integrity, confidentiality, etc.). The best algorithm of image encryption refers to the encrypted image that has a low correlation with the original image i.e. high imperceptibility for the encrypted image. The main challenges that face the designing of any algorithm of image encryption are; constructing a lightweight cryptographic algorithm without increasing the burden of

computation with a high number of encryptions, obtaining high imperceptibility for the encrypted image, getting faster response time for the encryption process, and retaining the highest level of image information in the decryption process [12].

Similar to the algorithms of cryptography, the lightweight cryptographic algorithms are also separated into two parts: symmetric and asymmetric algorithms [13]. Symmetric algorithms include stream and block ciphers. These ciphers are deliberately used with gadgets, and there are not any limitations for getting categorized as lightweight. Performance, cost, and security represent the main significant portions to deal with by every architect of lightweight cryptography. It is extremely hard to achieve the fundamental design aims: performance and security, cost and security, or performance and cost at the same time, whilst it is not difficult to develop any one of these aims. The symmetric ciphers' elements are entity authentication, encryption, checking message integrity, and etc., whilst the management of key and nonrepudiation are further functions supplied via asymmetric ciphers [14]. Lightweight Elliptic curve is asymmetric cipher that capable of ensuring both confidentiality and authentication, however, it requires more consumption of memory and larger size of key which led to make it less popular [15] [16].

The lightweight block cipher represents a complete data block that is processed at once. The main concerns for evaluating a lightweight block cipher are block size, key size, number of rounds, and the type of structure. While lightweight stream cipher works on encrypting and decrypting data bit by bit and it is quicker and simpler than lightweight block cipher [17]. In this paper, we will concentrate on some developed lightweight stream ciphers; Salsa20, and Chacha20, and their application in digital image encryption.

3. Developed Lightweight Algorithms for Image Encryption Application

Generally, the majority of current lightweight cryptography algorithms face the challenge associated with complexity, furthermore, their generated keys should be unpredictable. Regarding these concerns, further improvement on the generated keys can be added for making cryptographic algorithms high robustness against various kinds of cipher attacks. Recently, chaotic map systems paid considerable attention in several studies for the utilization of cryptographic applications owing to their properties of randomness [18].

The chaotic maps have different useful properties of application Depends on safety. These properties are; Chaos is a dynamic system in discrete time to produce in a complex sequence that conducts randomly in an easy and simple way, the chaotic signal is Non-random however but it is imperative, this feature allows us to renew it, the chaotic signal is very sensitive of the initial condition, this leads to another initial arrangement which makes another sequence. This property makes it so hard for the attackers to prophesy the chaotic chains to renew it and prevent attacks. The chaotic map functions are divided into two categories: 1-Dimensional and multilayered chaotic map functions [19]. These chaotic map systems can be utilized for generating pseudo-random keys to produce the developed lightweight cryptography algorithms. The general diagram of the developed lightweight (Salsa20 and Chacha20) algorithms for the application of digital image encryption is illustrated in Figure 1.

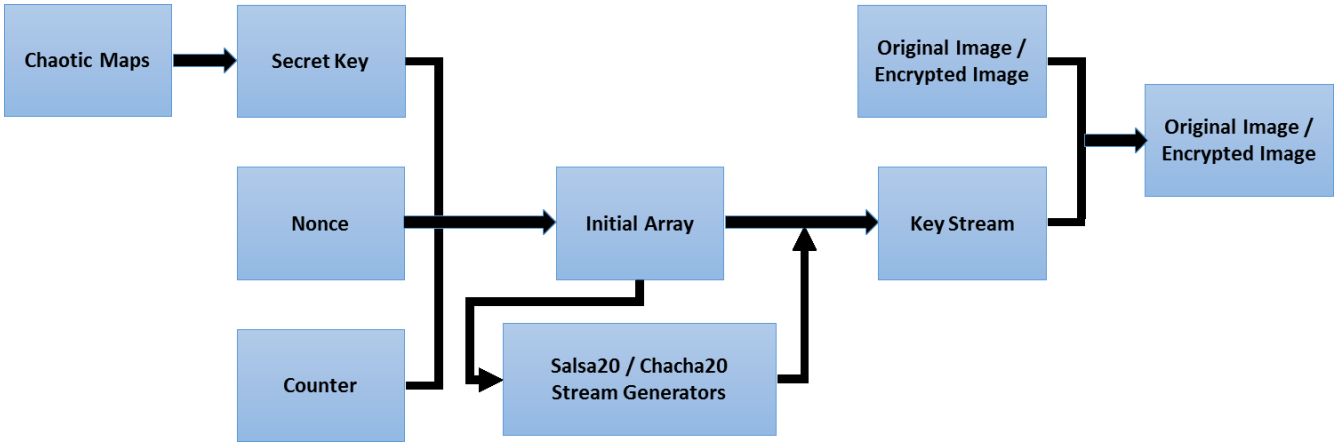

Figure 1. The general diagram of the developed lightweight Salsa20 / Chacha20 algorithms for image encryption/decryption.

3.1. Developed Lightweight Salsa20 Algorithm-Based Image Encryption

The stream cipher Salsa20 was presented via Bernstein [20]. It provides a clean, scalable, and very easy design, and offers 128, and 256 bits of keys in an extremely normal manner. The basic Salsa includes twenty rounds, however, subsequent Salsa includes eight rounds and twelve rounds. The original lightweight Salsa20 algorithm is constructed using a pseudorandom function depend on Add Rotate XOR operations. Hereafter, $\oplus$ indicates the bitwise XOR, $+$ indicates the addition modulo (2^{32}), || represents the concatenation, and $A<<<l$ indicates the l-bit left shift rotation on a word A. Salsa20 utilizes the counter mode hash function Salsa20. The keystream of 512 bits is generated with 64 bits counter and 64 bits' initial vector as inputs.

Salsa20 represents a stream cipher of word-oriented. Every word represents a component of $F2^{32}$ and includes 32 bits. At first, the Salsa20's round function is described using 4×4 matrix of words [21];

$$w = \begin{pmatrix} w_0 & w_1 & w_2 & w_3 \\ w_4 & w_5 & w_6 & w_7 \\ w_8 & w_9 & w_{10} & w_{11} \\ w_{12} & w_{13} & w_{14} & w_{15} \end{pmatrix} \quad (1)$$

The round function f(w) is given as follows;

$$f(w) = (Y'^4(w))^B \quad (2)$$

Where,

$$Y'(w) = \begin{pmatrix} w_5 & w_6 & w_7 & y_1 \\ w_9 & w_{10} & w_{11} & y_2 \\ w_{13} & w_{14} & w_{15} & y_3 \\ w_1 & w_2 & w_3 & y_0 \end{pmatrix}, \text{ and } y = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = Y \begin{pmatrix} w_0 \\ w_4 \\ w_8 \\ w_{12} \end{pmatrix}$$

The input of the Y function is four words, and the output is also four words, indicated by q= $q_0||q_1||q_2||q_3$ and r= $r_0||r_1||r_2||r_3$, respectively.

$$r_1 = q_1 \oplus ((q_0 + q_3) \lll 7)$$

$$r_2 = q_2 \oplus ((r_1 + q_0) \lll 9)$$

$$r_3 = q_3 \oplus ((r_2 + r_1) \lll 13)$$

$$r_0 = q_0 \oplus ((r_3 + r_2) \lll 18) \quad (3)$$

The function of encryption in Salsa20 is given as follows;

$$Salsa20_s(i,c) = H \begin{pmatrix} n_0 & s_0 & s_1 & s_2 \\ s_3 & n_1 & i_0 & i_1 \\ c_0 & c_1 & n_2 & s_4 \\ s_5 & s_6 & s_7 & n_3 \end{pmatrix} \quad (4)$$

Where, H indicates the hash function and it is computes as follows;

$$H(w) = w + f^f(w) \quad (5)$$

where $s = s_0||s_1|| \dots ||s_7$ denotes the secret key (256 bits), $i = i_0||i_1$ denotes the initial vector (64 bits), $c = c_0||c_1$ denotes the counter (64 bits), and $n = n_0||n_1||n_2||n_3$ denotes the constants (128 bits). If the length of the secret key is 128-bit, then the $(s_4, s_5, s_6, s_7) = (s_0, s_1, s_2, s_3)$ is approved.

The scalability and simplicity of Salsa20 have provided more significance in various applications, especially in image encryption. There are lots of works that have studied image encryption using several developed algorithms of Salsa20.

A. Jolfaei and A. Mirghadri [22], presented an effective implementation of a lightweight Salsa20 algorithm for the application of digital image encryption in which sequences of tests were accomplished for justifying the efficiency of Salsa20. The large key space of the Salsa20 algorithm enables it to resistant against all types of brute-force attacks, and the experimental results demonstrate that the lightweight algorithm has immunity against statistical attacks. The obtained results of chi-square and entropy tests demonstrate that the encrypted image was uniform and secure to entropy attack, respectively. Salsa20/8 is a fast algorithm and can provide a better quality of encryption than the Salsa20/12 and Salsa20/20. Finally, the Salsa20 algorithm represents a good applicant for image encryption.

M. Almazrooie et al. [23], presented a developed Salsa20 algorithm using a chaotic logistic map that requires only 2 rounds of scrambling for achieving a preferable level of diffusion to make the algorithm faster. The XOR operation was utilized for addressing the observed statistical leakage at the 2nd round of original Salsa20. According to the obtained results, this lightweight algorithm provides diffusion faster than the original Salsa20 and resists the known attacks.

A. H. Fadel et al. [24] proposed a developed lightweight Salsa20 algorithm for the application of digital image encryption which utilizes two chaotic maps (Logistic and Chebyshev maps) for achieving diffusion faster than the original Salsa20 algorithm. This developed algorithm consists of several stages; firstly, the generation of the random sequence using the chaotic maps, secondly, the expansion of the key, and lastly, the encryption and decryption of images using XOR operation. The pixels' distribution within the histogram of the encrypted image was uniform and considerably different from the original image. The obtained results demonstrate that the proposed light weight algorithm is more efficient, secure, and holds less complexity than the traditional Salsa20.

E. L. Mohaisen and R. S. Mohammed [25], proposed a developed lightweight Salsa20 algorithm based on a set of chaotic maps for achieving more complexity. This developed algorithm is utilized for encrypting and decrypting texts, gray, and color images. The obtained encrypted

images were uniform and extremely different from the original images, which refer to the efficiency of the developed Salsa20 algorithm.

K. R. Qasim and S. S. Qasim [26], presented a developed Salsa20 algorithm based on chaos theory for achieving faster propagation comparing with the original algorithm. The proposed algorithm was implemented on the medical images for providing more confidentiality for patients' diseases. It includes two main stages; firstly, the generation of a random key by utilizing the algorithm of Salsa 20 and the logistic map, then, the encryption and decryption of the medical images. Lots of tests were performed on the encrypted images for justifying the visual efficiency of the proposed Salsa20 algorithm. The obtained results demonstrate that the proposed algorithm was faster than other versions of Salsa20, and it has high resistance against various attacks.

3.2. Developed Lightweight Chacha20 Algorithm-Based Image Encryption

The encryption algorithm Chacha20 is a lightweight algorithm that belongs to the Salsa algorithm family but differs in detail. Chacha20 provided the best security than the original Salsa20 cipher, via utilizing somewhat preferable hash functions. The hash function input data rearranged for implementing the algorithm effectively [27].

The stream cipher Chacha20 algorithm works on 64 bytes of data blocks. The ChaCha20 algorithm calls the function of expansion to every 64 bytes of the data block. The input to this function represents a secret key of 32,16, or 8 bytes, furthermore, related to the number of the presently encrypted block. The essence of the lightweight Chacha20 algorithm is concentrated on utilizing the function of mixing that takes 64 bytes from the function of expansion, after that, combines these bytes, and lastly yields other 64 bytes of data to the function of expansion. The function of mixing works on data separated into 32-bit words ordered in a 4×4 matrix. The input matrix w is given as follows [28]:

$$w = \begin{pmatrix} w_0 & w_1 & w_2 & w_3 \\ w_4 & w_5 & w_6 & w_7 \\ w_8 & w_9 & w_{10} & w_{11} \\ w_{12} & w_{13} & w_{14} & w_{15} \end{pmatrix} \quad (6)$$

The fundamental role of the ChaCha20 algorithm is given to the QuarterRD function in which four words (e; f; g; h) are taken as input and four words are obtained as output after implementing the following operations of 32-bit:

$$e+= f; h \oplus= e; h <<<= 16;$$

$$g+= h; f \oplus= g; f <<<= 12;$$

$$e+= f; h \oplus= e; h <<<= 8;$$

$$g+= h; f \oplus= g; f <<<= 7; \quad (7)$$

The DoubleRd function is called within the function of mixing that accepts matrix w as input and results another matrix;

$$\boldsymbol{y} = DoubleRd\,(w) = DiagonalRD(ColumnRD(w)) \quad (8)$$

Where, the function QuarterRD is called four times by the function ColumnRD(x), once for every column of matrix w. Also, the function QuarterRD is called by the function of DiagonalRD(w) four times, one time for every diagonal of matrix.

Since the ChaCha20 algorithm considers a relatively new lightweight stream algorithm, therefore, there are no much researches in the literature working on the application of digital image encryption. Here, we can mention a developed lightweight ChaCha20 algorithm using hyperchaotic maps in the application of digital image encryption proposed by M. S. Mahdi et al. [29]. This developed lightweight algorithm for image encryption has achieved robustness to brute force attacks via supplying a massive space of keys. Several criteria were utilized in this algorithm for defense from statistical cracking and non-security of images. Furthermore, this developed ChaCha20 algorithm can run in real-time since it requires about 3.5 seconds consuming time.

4. Performance Analysis

The need for transferring digital images with large sizes has been growing. Therefore, securing these images needs holding algorithms that are capable of encrypting images at a high speed. Salsa20 and Chacha20 are stream ciphers that can be implemented in applications where the encryption speed is as important as the security. This review paper works on investigating the efficiency of utilizing the chaotic maps with the lightweight stream cipher algorithms (Salsa20

and Chacha20) for encrypting the images. Table 1 explains a comparison between the developed lightweight (Salsa20 and Chacha20) algorithms for the application of digital image encryption.

Table 1. Comparison between the developed lightweight stream ciphers for the application of digital image encryption.

Authors Name, Ref. No., Year	The Utilized Algorithms	Performance
A. Jolfaei and A. Mirghadri [14], 2010	Original Salsa20/8, Salsa20/12, and Salsa20/20.	Salsa20/8 is faster and has a better quality of image encryption than Salsa20/12, and Salsa20/20
M. Almazrooie et al. [15], 2015	Lightweight Salsa20 based on chaotic logistic map.	The lightweight algorithm provides diffusion faster than the original Salsa20 and resists the known attacks.
A. H. Fadel et al. [16], 2020	Lightweight Salsa20 algorithm based on Logistic and Chebyshev maps.	This algorithm is more efficient, secure, and holds less complexity than the original Salsa20.
E. L. Mohaisen and R. S. Mohammed [17], 2020	Lightweight Salsa20 algorithm based on a set of chaotic maps.	The obtained encrypted images were uniform and extremely different from the original images.
K. R. Qasim and S. S. Qasim [18], 2020	Salsa 20 based on logistic map.	The algorithm is faster than other versions of Salsa20, and it has high resistance against various attacks.
M. S. Mahdi et al. [21], 2020	lightweight ChaCha20 algorithm based hyperchaotic maps.	This developed algorithm has robustness to brute force attacks and can run in real-time.

5. Conclusions

Regardless of security concerns, there is another problem with the encryption of digital images that is significant as well. This involves the speed of the image encryption in real-time. Generally, the speed of the image encryption is extremely based on several concepts such as; the size of memory, the structure of CPU, the programming language, and etc. Therefore, it is useless to compare the speed of image encryption algorithms unless utilizing the same developed environment. in this review paper, in spite of this indicated problem, for demonstrating the efficiency of the developed lightweight cryptographic algorithms, a comparison between the presented algorithms were done in a brief manner.

References

[1] Mohamed Z. T., Xingyuan W., "A new fractional one dimensional chaotic map and its application in high-speed image encryption", Information Sciences, Vol. 550, (2021), 13-26.

[2] Mazher, A., Waleed, J., & MaoLood, A. (2020). The Security Threats and Solutions of Network Functions Virtualization: A Review. Journal of Al-Qadisiyah for Computer Science and Mathematics, 12(4), Comp Page 38-50.

[3] Najeeb, H. (2020). Steganography Technique for Embedding a Variety of Binary Images inside a Grayscale Image. Journal of Al-Qadisiyah for Computer Science and Mathematics, 12(2), Comp Page 1 -11.

[4] Waleed J., Jun H. D., Abbas T., Hameed S., Hatem H. (2014). A Survey of Digital Image Watermarking Optimization based on Nature Inspired Algorithms NIAs. International Journal of Security and Its Applications, 8(6), Page 315-334.

[5] Waleed J., Jun H. D., Hameed S. (2015). An Optimized Digital Image Watermarking Technique Based on Cuckoo Search (CS). ICIC Express Letters Part B: Applications. 6(10), Page 2629-2634.

[6] J.S. Al-janabi, R., J.S. Al-janabi, S., & Hussein Toman, Z. (2017). New method for Increasing watermarked image quality and security. Journal of Al-Qadisiyah for Computer Science and Mathematics, 9(2), Comp Page 78 - 85.

[7] Abduldaim A. M., Waleed J., Mazher A. N. (2020). An Efficient Scheme of Digital Image Watermarking Based on Hessenberg Factorization and DWT. 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, Page 180-185.

[8] Sabri R. I., Abduldaim A. M., Waleed J. (2020). Mamdani FIS Combined With LU Decomposition Method and Two-Level LWT for Image Watermarking Technique," 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), Najaf, Iraq, Page 12-17.

[9] Ahmed, A., Salah, H., & Jameel, J. (2019). Multikey Image Encryption Algorithm Based on a High-Complexity Hyperchaotic System. Journal of Al-Qadisiyah for Computer Science and Mathematics, 11(3), Comp Page 69-85.

[10] Rokan Naif, J., H. Abdul-majeed, G., & K. Farhan, A. (2019). Internet of Things Security using New Chaotic System and Lightweight AES. Journal of Al-Qadisiyah for Computer Science and Mathematics, 11(2), comp 45-52.

[11] A. N. Mazher and J. Waleed, " Implementation of Modified GSO Based Magic Cube Keys Generation in Cryptography", Eastern-European Journal of Enterprise Technologies, vol. 1, No. 9-109, (2021), 43-49.

[12] Maniyath S.R., Thanikaiselvan V., "Robust and Lightweight Image Encryption Approach Using Public Key Cryptosystem", Cybernetics and Algorithms in Intelligent Systems. CSOC2018 2018. Advances in Intelligent Systems and Computing, Vol. 765. Springer, Cham, (2019), 1-11.

[13] T. M. Hasan, J. Waleed, N. M. Sahib, "Information Hiding Based on Retina Random Number Keys", Solid State Technology, Vol. 63 No. 1 (2020), 497-787.

[14] Shah A., Engineer M., "A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications", Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing, Vol. 851. Springer, Singapore, (2019), 283-293.

[15] N. Raad, T. Hasan, A. Chalak and J. Waleed, "Secure Data In LoRaWAN Network By Adaptive Method Of Elliptic-curve Cryptography", 2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA), (2019), 1-6.

[16] N. Raad, T. M. Hasan, A. Chalak and J. Waleed, "Secure Data Transmissions for Iraqi National Identification Card Using LoRaWAN Protocol", 2019 2nd International Conference on Engineering Technology and its Applications (IICETA), (2019), 67-72.

[17] Muhammad Rana and Q. Mamun and M. R. Islam, "Current Lightweight Cryptography Protocols in Smart City IoT Networks: A Survey", ArXiv, Vol. abs/2010.00852, (2020), 1-22.

[18] Z. M. Jawad Kubba and H. K. Hoomod, "A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System," 2019 First International Conference of Computer and Applied Sciences (CAS), (2019), 199-203.

[19] H. A. Ismael, J. M. Abbas, S. A. Mostafa, and A. H. Fadel, “An enhanced fireworks algorithm to generate prime key for multiple users in fingerprinting domain,” Bull. Electr. Eng. Informatics, Vol. 10, No. 1, (2020), 337–343.

[20] D. J. Bernstein, "The Salsa20 Family of Stream Ciphers", New Stream Cipher Designs. Lecture Notes in Computer Science, vol. 4986. Springer, Berlin, Heidelberg, (2008), 84–97.

[21] Lin Ding, "Improved Related-Cipher Attack on Salsa20 Stream Cipher", in IEEE Access, Vol. 7, (2019), 30197-30202.

[22] A. Jolfaei and A. Mirghadri, "Survey: Image Encryption Using Salsa20", IJCSI International Journal of Computer Science Issues, Vol. 7, No. 5, (2010), 213-220.

[23] M. Almazrooie, A. Samsudin, M. M. Singh, "Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map", Journal of Information Processing Systems, Vol. 11, No. 2, (2015), 310-324.

[24] A. H. Fadel, R. S. Hameed, J. N. Hasoon, S. A. Mostafa, B. A. Khalaf, "A Light-weight ESalsa20 Ciphering based on 1D Logistic and Chebyshev Chaotic Maps", Solid State Technology, Vol. 63, No. 1, (2020), 704-717.

[25] E. L. Mohaisen and R. S. Mohammed, "Improving Salsa20 Stream Cipher Using Random Chaotic Maps," 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), (2020), 1-6.

[26] K. R. Qasim, and S. S. Qasim, "Encrypt Medical Image using CSalsa20 Stream Algorithm", Medico-Legal Update, Vol. 20, No. 3, (2020), 1248-1256.

[27] S. Dey, and S. Sarkar, "Improved analysis for reduced round Salsa and Chacha", Discrete Applied Mathematics, Vol. 227, (2017), 58-69.

[28] A. Czubak, A. Jasiński, M. Szymanek, "A Note on Keys and Keystreams of Chacha20 for Multi-Key Channels", Computer Networks, Communications in Computer and Information Science, Vol. 860. Springer, Cham, (2018), 1-16.

[29] M. S. Mahdi, R. A. Azeez, N. F. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps", Periodicals of Engineering and Natural Sciences, Vol. 8, No. 4, (2020), 2138-2145.