JOIV : Int. J. Inform. Visualization, 8(2) - May 2024 977-982

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Lightweight Image Encryption Based on A Hybrid Approach

Alaa A. Jabbar Altaay [a,*], Jamal N. Hasoon [a], Hassan Kassim Albahadily [a]

[a] *Computer Science Department, University of Mustansiriyah, Falastin St, Baghdad, 10052, Iraq*

Corresponding author: [*]alaaaltaii.phd@uomustansiriyah.edu.iq

***Abstract*—A secure image could be achieved by encryption, a technique for securing images over different media transmission lines with privacy and keeping them safe for the receiver. This paper proposes an image encryption approach to achieve excellent security by combining a lightweight encryption algorithm with the chaotic Peter De Jong map. The Lilliput algorithm, lightweight encryption, uses the Peter De-Jones map to produce keys. The suggested approach achieved a suitable level of complexity that matched the historical demands for transmission images. Two methods were used to conduct the tests on a standard image collection: an encrypted image and a generated key. Standard metrics find the similarity between the input and output images to achieve an accurate proposal performance. The encrypted image's entropy was assessed and discovered that it matched the original image values exactly. The results were satisfactory regarding obtaining a precise correlation rate between the original and encrypted photos. The decryption and reconstruction of the image were completed quickly and steadily, with a high success rate and excellent outcomes. The proposed approach was evaluated on a dataset of well-known test photos with unique features, including varying degrees of lightness and shade to create the perfect test.**

***Keywords*—Chaotic map; lilliput lightweight encryption method; chacha20-hash function.**

Manuscript received 5 Nov. 2023; revised 7 Jan. 2024; accepted 19 Feb. 2024. Date of publication 31 May 2024.

I. Introduction

Data encryption is one of the most critical areas in information and communication technology, which shields data from alteration or manipulation to prevent security breaches. Additionally, as technology has advanced, image encryption has become popular due to concerns about user privacy [1] and the fact that information security should always be considered [2]. The two forms of encryption are block ciphers and stream ciphers; the stream cipher algorithms encrypt the message using a secret key generator mechanism. The same algorithm decrypts the message using the same encryption technique [3], and the stream cipher, such as non-linear combination generators, shift registers, etc., could be used to produce a key for encrypting the messages. A set of stream cipher algorithms has been utilized [4]. The block cipher converts a whole data block at once [5]. Various algorithms of block cipher have been used, including Salsa [6], Rabbit [7], and HC128 [8].

In addition, it is according to the key that is used in the cryptosystem. The symmetric method uses one key in encryption and encryption between the sender and the recipient in secret key cryptosystems. Conversely, in public-key cryptosystems, a private key is used to decode the cipher text after plaintext has been encrypted with a public key [9]. Chaos theory has been used in a variety of disciplines, including biology, and found a close correlation between the concepts of chaos and cryptography [10]. The chaotic technique is strongly related to cryptography because of the significant pixel correlations and real-time processes required by multimedia [11]. This is because real-time systems that use lightweight encryption need it to maintain perceptual information [12], [13].

Much research has examined the encryption process using mathematical application models for chaotic systems, including the logistic, Henon, Rossler, Lorenz, and Peter de Jong maps [14]. The beginning states, control parameters for the circumstances, randomization properties, and transitivity in the system behavior are some of the features of chaotic systems [15], [28]. The chaotic map and Lightweight Encryption applied in various research have been utilized in the following paragraphs. Several works use the chaotic system, such as Chenghai et al. [16]. The suggested RGB picture encryption technique verifies that employing chaotic maps to encrypt an image satisfies safe cipher diffusion and confusion requirements. Furthermore, the key sequence to encrypt the photos is also constructed using a mix of Sine

chaotic maps and 1D logistic maps. The suggested method offers respectable security against various assaults and a large secret key space, as exposed by the experimental and compassionate results, Khan et al. [17] suggested a hyperchaotic system. This novel color image encryption technique employs the "transforming-scrambling-diffusion" concept. The color image's pixel values were continuously changed to produce the grey image. The chaotic sequence was then constructed using a 4D hyperchaotic system transformed into a vector.

Finally, the generated numbers were sorted for reorder, and the matrix was done. Image diffusion was accomplished via a bit-operation. The information entropy, correlation, key sensitivity, histogram, and other evaluation indices were calculated throughout the experiment. According to the findings, the encryption algorithm is very resistant to assaults. Yassin et al. [18] proposed combining Brownian motion with unique ternary orientation connected to random movement over time and spatial coordinates. A chaotic dynamical map has been employed to offer another level of security to the suggested encryption system. The recommended approach was evaluated using a set of statistical tests, and it was found to outperform existing image encryption algorithms in terms of security. Masood et al. [19] suggested utilizing the Cha-cha as a stream cipher using a Hyperchaotic Map for crucial generation to create an encrypted image. The adaptive security that changes over time could be satisfied when changing the seed numbers, initial parameters, and control parameters.

Furthermore, the proposed method has shown resilience against brute force assaults by offering a large critical space. Jannatul et al. [20] described a method for encrypting data based on double chaotic systems. This method uses system behavior (chaotic system) presented maps, which involve pixel shuffling with replacement processes, to complete the two-process confusion and diffusion. This hybrid method divides the original image into sub-bands using a mixture of Discrete Wavelet Transforms (DWT). The suggested technique works effectively and is resistant to a range of common assaults, as shown by test analysis and comparisons with other methods, Hui et al. [21] proposed a secure processing technique that is more reasonably priced. The key to the system is fractals and the three-dimensional Lorenz chaotic map, which are used in a shuffling method. The shuffling resulted in jumbled pixels in the image, contributing to the disorientation feature. A 3D Lorenz system uses an encryption process (diffusion process) to replace the data representing the image pixel.

Throughout the security test, the entropy levels for each grey channel were close to the optimal value, Yucheng et al. [22] suggested a low-power encryption method to safeguard cloud apps that used 128-bit key and 128-bit block size and the logical operations with shifting and substitution, the select key length depends on number of spins required in algorithm. Thabit et al. [23] suggested a straightforward message-passing algorithm and chaotic map message for image encryption. Important messages may be communicated locally to the message-passing (MP) technology, which enables free interaction between adjacent pixels. This chaotic system may quickly produce pseudorandom sequences of excellent quality. The external message sets of edge pixels are generated through a pseudorandom sequence generator, a two-dimensional logistic map. An encrypted image can be created by modifying edge pixels by interacting with one another in the external message. As such, the cipher image has sufficient information entropy and uniform distribution. Additionally, the suggested approach lowers correlation coefficients and covers all plain-image characters.

Chai et al. [24] proposed to encrypt images using a unique chaotic image encryption strategy based on DNA sequence operations by first randomizing image pixels employing a CML-linked map and then encoding the image employing DNA encoding. This approach combines DNA encoding with a chaotic system. The suggested system is safe enough to withstand known assaults and has a strong encryption effect, according to experimental findings and security studies. Berger et al. [25] developed a permutation-diffusion structure based on the standard map and the piecewise linear chaotic map (PWLCM) used in an encryption technique. The permutation phase uses a hierarchical diffusion methodology, which modifies the pixel position and value instead of the standard scrambling method. The row-by-row and column-by-column operation models are also used to increase the diffusion process's efficiency further. Consequently, one may achieve a fair trade-off between security and efficiency.

A. Peter De Jong Attractor

The Peter De Jong map is a two-dimensional iterative chaotic system of differential equations that displays a series of complex attractors that correlate to the input arguments related to attractors. The initial parameters provide sensitivity to the chaotic system described by these equations.

$$Xn+1=sin(ayn)-cos(bxn) \quad (1)$$

$$Yn+1=sin(cyn)-cos(dxn) \quad (2)$$

The values of x_n, and y_n give the next two values x_{n+1}, and y_{n+1} using the parameters (a, b, c, and d) as control parameters for a chaotic system. Initially, a rectangular section of the plane spanning the image needs to be identified. A group of discrete pixels must be selected. Next, compute several map iterations and count the times to contact every pixel. The chaotic output sequence's mean and self-correlations should then be calculated. A series of forms from the Peter De Jong map [26] are explained in Fig. 1.

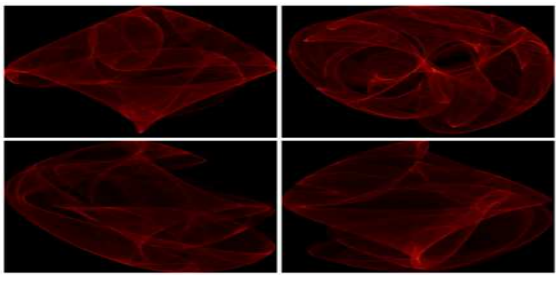

Fig. 1 Some samples of Peter De Jong attractor [26]

B. LILLIPUT Encryption Method

At the nibble level, LILLIPUT uses a type of Feistal Network called EGFN with a 64-bit and around function as a block cipher technique with an 80-bit key. The X is represented by sixteen bits. X0 through X15 are the codes

for these bits. It consists of thirty rounds, or thirty iterations of a single EGFN termed OneRoundEGFN; in (3), the range of each Fi for i is 0 to 7.

$$Fi = S\,(X7{-}i \oplus RKi) \tag{3}$$

where S is an S-box functioning at the nibble level, and RKi is the nibble at position I of the 32-bit subkey RKj of round j. The critical schedule divides the passkey into thirty 32-bit subkeys or RKj. It is important to remember that there was no permutation layer in the last round due to involution. In Fig. 2, the encryption procedure is displayed [27].

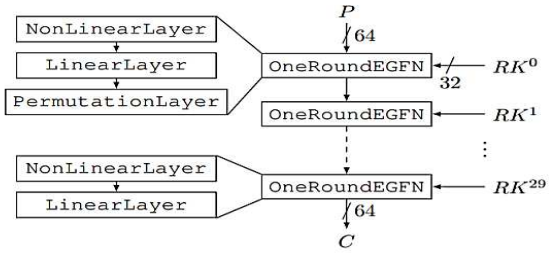

Fig. 2 Block Diagram of LILLIPUT Enc. Method [27]

The thirty subkeys, RK0 to RK29, are created from the passkey K using the key schedule depicted in Fig. 3, which facilitates on-the-fly computations. It uses an 80-bit linear finite state machine (LFSM) [28]. Its internal state is represented by the letter Y, and the passkey K initiates it. ExtractRoundKey, a layer of parallel S-boxes, is used to extract the subkeys from the LFSM state Y. In the LFSM starting state, the passkey K, or subkey RK_0, is deleted. The subkeys are extracted from the LFSM state Y using ExtractRoundKey, a layer of parallel S-boxes. The passkey K, or subkey RK^0, is eliminated in the LFSM initial state. RoundFnLFSM is then used to update the LFSM state Y, and RK^1, the following subkey, is retrieved [29].

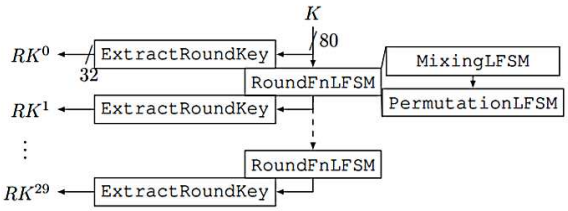

Fig. 3 Key Schedule [27]

Until RK^{29}, twenty bits make up the state Y: Y_{19}, Y_0, which are split among four LFSRs, L_0 to L_3, each of which operates on five nibbles: L_0 operates on Y_0 to Y_4, L_1 operates on Y_5 to Y_9, and so on, see Fig. 4. Make use of LFSRs inspired by LFSR findings. LFSRs inspired by LFSR findings should be used. More precisely, it is possible to create a Feistel representation that generalizes the usual Fibonacci and Galois terms, matching the matrix representation seen in word-oriented LFSRs with word feedback that has been carefully crafted to match. Moreover, the feedback is computed using simple word-oriented operations like rotations and shifts.

Those structures' two main benefits are a simple reversal and a noticeable acceleration of diffusion. Operating on five nibbles, The LILLIPUT key schedule's four LFSRs are Feistel-like and word-oriented. A detailed list can be seen below (for a visual depiction) [30]. As a result, two transformations of the RoundFnLFSM function represented by four Feistel-like word-oriented LFSRs in Fig. 4 may be distinguished: Permutation LFSM, which is the word-wise cyclic shift, and MixingLFSM, which maintains the feedback element.

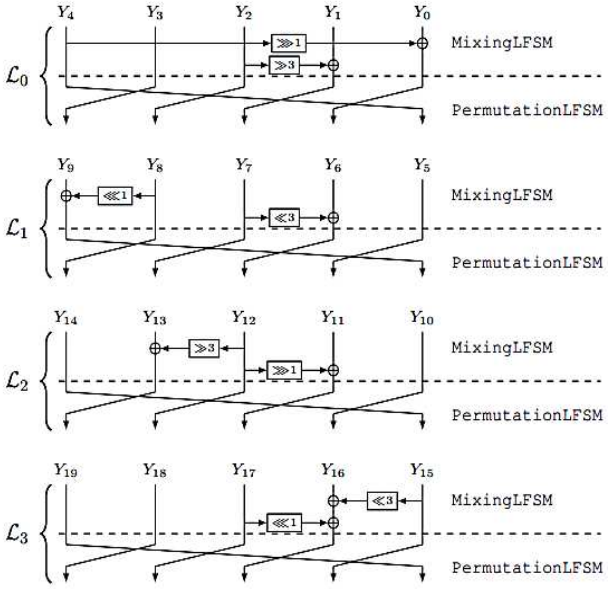

Fig. 4 LFSRs L0 to L3 are used in the key schedule [27]

II. Material and Method

A method of combining dynamic key generation with an encryption algorithm (lightweight) in an effective schema is proposed. A three-stage generation of the required number is represented by: the first series is used to permute the image's pixels; in the second, the block to be encrypted is chosen, resulting in a non-linear process; and in the third, new keys are created by determining a relationship between the first and second sequences., which is used in the proposed encryption Lilliput algorithm as shown in Figure 5.

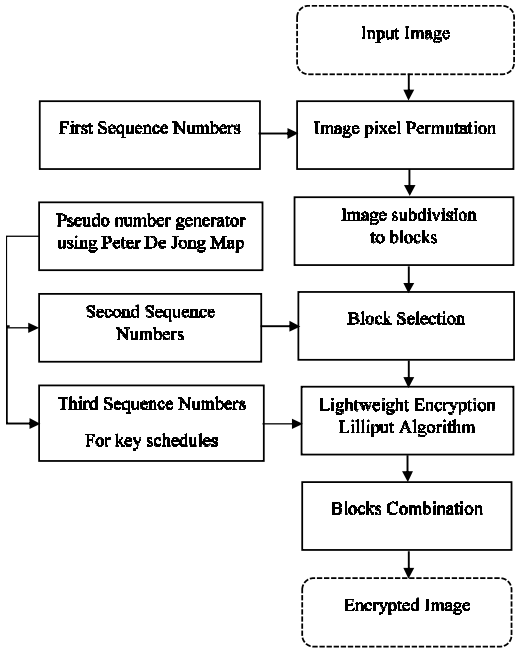

Fig. 5 The Framework of the Proposed Method

C. Key Generation using Peter De Jong Map

This study uses a key generation approach based on the De Jong map, a two-dimensional chaotic function, as two numbers are created at each step. The image pixels are permuted in rows and columns using the first series. The procedure is non-linear because the block to be encrypted is chosen in the second series. The first and second series are linked simultaneously to create the third series, which serves as keys for encrypting the blocks.

The produced numbers are actual numbers in the interval (0,1) that have been absolute, stripped of floating points, and concatenated to form a series. The second dimension of the produced numbers is then processed using the same procedures. The third series is then formed by exclusivity or by placing every bit from series one in the same location as series two, depending on the preceding two series.

D. Image Pixel Permutation

This stage involves redistributing the image's pixels to create a randomly dispersed collection, altering the image's characteristics, and adding complexity to the process. Using this approach, a collection of numbers from the first series is sorted, either ascending or descending, so that the total number of rows is equal. These integers' placements serve as a permutation key. Another generated set of numbers is selected and similarly sorted in the columns. The two variations of the rearranged image Lenna are shown in Figure 6.

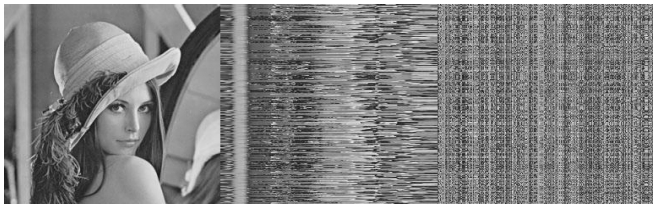

Fig. 6 Test image Lenna with its permutation row and column

E. Block Partitioning

As seen in Figure 7, the permuted image is divided into blocks of the same length as the blocks input into the recommended encryption method (Lilliput method).

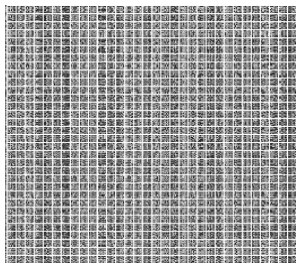

Fig. 7 The Image Subdivided Blocks

F. Block Selection

When a set of numbers equal to the entire number of blocks is obtained, it is multiplied by the number of total blocks to acquire a decimal number, which is then used to choose blocks from the second series of generated numbers. As shown in Figure 8, these numbers provide a unique key index for the selected block.

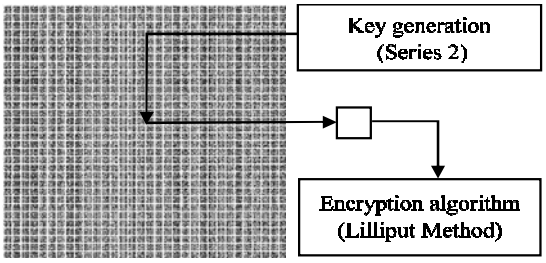

Fig. 8 Block Selection

G. Lightweight Encryption Lilliput Algorithm

The image's blocks are all resized into vectors and transformed into hexadecimal representations. Each block has a subsequence of 20 hexadecimal digits from the key sequence delivered for encryption. The created key creates a new arrangement based on the exclusive or both sequences obtained using the suggested pseudo number generator approach.

H. Blocks Combination

The encrypted image resulting from the suggested approach is rebuilt by concatenating the ciphered blocks. To provide strong security and enhance complexity, every encrypted block is created non-sequentially using a new matrix based on the new locations.

III. Results and Discussion

This section discusses the experimental outcomes of using the suggested strategy. Experiments using the proposed technique have been conducted on standard photographs with different color gradations, as shown in Figure 9.

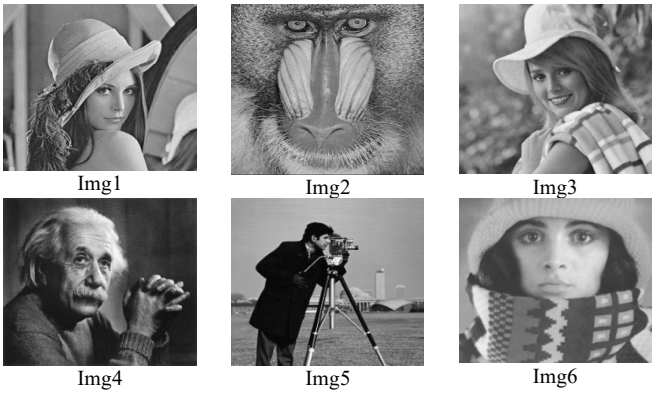

Fig. 9 The Test Images Used in The Experiment

The critical space analysis prevents the so-called brute force attack; the critical space should be greater than 2^{128}, while the size of the generated key depends on a set of initial factors, which are the value of the constants a, b, c, and the initial values of x and y. The critical space is found from the initial parameters, where the precision of each is 10^{10}. Therefore, it is calculated as $(10^{10})^6 \approx 2^{199}$, which means that sizeable critical space denotes that the encryption scheme can withstand brute-force attacks.

The NIST tests were applied to evaluate the efficiency of generated numbers. The accurate randomness archived was compared to the algorithm's findings to verify that the suggested key generation has excellent security and is resistant to attacks.

The correlation checks findings for every image shown in Table 1 for those used to assess the outcomes. Before and after the encryption procedure, examine the relationship between these images in the diagonal, horizontal, and vertical directions. It is observed that there is a strong connection (almost one) between images before encryption. Due to the connection breakdown, these numbers were no longer near zero or negative values in either direction.

TABLE I
THREE TYPES OF CORRELATION (VERTICAL, HORIZONTAL, AND DIAGONAL)

	Original images			Encrypted images		
#	Vertical	Horizontal	Diagonal	Vertical	Horizontal	diagonal
1	0.946	0.972	0.916	-0.007	-0.024	0.016
2	0.861	0.806	0.760	0.019	-0.019	0.002
3	0.975	0.985	0.951	-0.003	-0.021	0.010
4	0.976	0.983	0.954	-0.018	0.006	0.006
5	0.946	0.968	0.920	0.007	-0.025	-0.007
6	0.989	0.989	0.972	0.001	-0.001	0.005

Several objective techniques are available to determine how similar two photos are. Several tests may be employed to determine how different they are from one another. The quality of the suggested photos is evaluated by contrasting them with the original photographs. The findings have been accepted because the encrypted image does not resemble the original image. After encryption, the entropy test is performed, and the results may be similar to the previous value. Ultimately, the quality of the encrypted photos was verified by comparing them to the original and determining the difference.

IV. CONCLUSION

The primary goal of encrypting the image's data is to protect it while it is being sent, stored, and retrieved. This paper presents a technique for image encryption. This gives more secrecy by suggesting an efficient method combined with a specific key generation and a lightweight encryption technique (LILLIPUT). The randomness test was applied to the generated number to gauge how effective the suggested procedure was—the quality of the images obtained after the encryption procedure was examined and contrasted with the original. The correlation of images was disconnected. The entropy of the image was evaluated after encoding, and the results were highly efficient. Additionally, the degree of departure from the original image was calculated, and the image quality was assessed using predetermined standards. This computation relies on these metrics to determine the image's degree of similarity to the original. Testing revealed no correlation between the encrypted image quality and the input image quality. Multiple tests are used in method experiments to determine performance metrics.

Finding a high percentage of correlation between the original and encrypted images was one of the more pleasing outcomes that might be attained. Decryption and reconstruction of the image were fast and stable, and a high percentage of success and high results were achieved.

The suggested method was tested on a dataset of famous test images with unique characteristics like different levels of lights and shades to make an ideal test on these images. Additional studies using different video file formats, text data, databases, etc., could use the proposed approach. It may be integrated with another lightweight encryption technique or used as a complete key creation method.

REFERENCES

[1] H. Tayyeh, M. Mahdi, A. AL-Jumaili, "Novel steganography scheme using Arabic text features in Holy Quran," International Journal of Electrical and Computer Engineering, vol. 9, No. 3, pp. 1910-1918, 2019.

[2] M. Mahdi, N. Hassan, "A proposed lossy image compression based on a multiplication table," Kurdistan Journal of Applied Research (KJAR), vol. 2, No. 3, pp. 98-102, 2017.

[3] M. Mahdi, N. Hassan, "Design of keystream Generator utilizing Firefly Algorithm," Journal of Al-Qadisiyah for computer science and mathematics, vol. 10, No. 3, pp. 91, 2018.

[4] A. Kadhim, M. Salih, "Proposal of new keys generator for DES algorithms depending on multi techniques," Engineering and Technology Journal, vol. 32, No. 1, pp. 94-106, 2014.

[5] D. Salman, R. Azeez, A. Abdul-hossen, "Build Cryptographic System from Multi-Biometrics using Meerkat Algorithm," Iraqi Journal for Computers and Informatics, vol. 45, No. 2, pp. 1-8, 2019.

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

[7] M. Mahdi, N. Hassan, "A Suggested Supper Salsa Stream Cipher," Iraqi Journal for Computers and Informatics (IJCI), vol. 44 No. 2, 2018.

[8] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, O. Scavenius, "Rabbit: A new high-performance stream cipher," International Workshop on Fast Software Encryption, vol. 2887, pp. 307– 329, 2003.

[9] H. Azeez, A. Mohammed, "New Encryption Algorithm Using Block Concept," Design Engineering, vol. 7, 2021.

[10] M. Mahdi, R. Azeez, N. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," Periodicals of Engineering and Natural Sciences, vol. 8, No. 4, pp. 2138-2145,2020.

[11] A. Jabbar, S. Sahib, M. Zamani, "Pixel Correlation Behavior in Different Themes," International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem (GRMSE2013), vol. 398, 2013.

[12] D. Salman, R. Azeez, A. Hossen, "Key generation from multibiometric system using meerkat algorithm," Engineering and Technology Journal, vol. 38, No. 3B, pp. 115-127, 2020.

[13] A. Jabbar, S. Sahib, M. Zamani, "Correlation Analysis of the Four Photo Themes in Five Layers", International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem (GRMSE2013), vol. 398, 2013.

[14] I. Taqi, Hameed S., "A new Color Image Encryption based on multi–Chaotic Maps," Iraqi Journal of Science, vol. 59, No. 4B pp. 2117-2127, 2018.

[15] S. Mahmood, K. Hussein, Y. Jurn, E. Albahrani, "Parallelizable cipher of color image based on two-dimensional chaotic" Indonesian Journal of Electrical Engineering and Computer Science vol. 18, No. 1, April 2020, pp. 101~111.

[16] L. Chenghai, Z. Fangzheng, L. Chen, Z. Jie, "A Hyperchaotic Color Image Encryption Algorithm and Security Analysis," Security and Communication Networks, vol. 2019, Article ID. 8132547.

[17] M. Khan, F. Masood, A. Alghafis, M. Amin, N. Batool, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," PLoS One, vol. 14, No. 12, 2019.

[18] A. Yassin, A. Rashid, A. J. Yassin, H. Alasadi, "A novel image encryption scheme based on DCT transform and DNA sequence," Indonesian Journal of Electrical Engineering and Computer Science vol. 21, No. 3, March 2021, pp. 1455~1464.

[19] F. Masood, J. Ahmad, S. Shah, S. Jamal, I. Hussain, "A novel hybrid secure image encryption based on Julia set of fractals and 3D Lorenz chaotic map," Entropy, vol. 22, No. 3, 2020.

[20] F. Jannatul, B. Mahbuba, S. Mohammad, "Chaotic Lightweight Cryptosystem for Image Encryption," Advances in Multimedia, vol. 2021, pp. 1-16, 2021.
[21] L. Hui, Z. Bo, Z. Jianwen, H. Linquan, L. Yifan, "A Lightweight Image Encryption Algorithm Based on Message Passing and Chaotic Map," Security and Communication Networks, vol. 2020, No. 4, pp. 1-12, 2020.
[22] C. Yucheng, T. Chunming, Y. Zongxiang, "A Novel Image Encryption Scheme Based on PWLCM and Standard Map," Complexity, vol. 2020, pp. 1-23, 2020.
[23] F. Thabit, S. Alhomdy, A. Al-Ahdal, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," Global Transitions Proceedings 2, pp. 91-99, 2021.
[24] X. Chai, Z. Gan, K. Yuan, Y. Chen, X. Liu, A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Computing and Applications, vol. 31, pp. 219-237, 2019.
[25] T. Berger, J. Francq, M. Minier, G. Thomas, "Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher," IEEE Transactions on Computers, vol. 65, No. 7, pp. 1-17.
[26] T. Berger, M. Minier, B. Pousse, "Software oriented stream ciphers based upon FCSRs in diversified mode," International Conference on Cryptology in India, pp. 119-135, 2009.
[27] F. Arnault, T. Berger, M. Minier, B. Pousse, "Revisiting LFSRs for cryptographic applications," IEEE Transactions on Information Theory, vol. 57, No. 12, pp. 8095-8113, 2011.
[28] X. Li, C. Li, I. Lee, “Chaotic image encryption using pseudo-random masks and pixel mapping,” Signal Processing, Vol. 125, pp. 48-63. 2016.
[29] R. Guesmi, B. Farah, A. Kachouri, M. Samet. “Hash key based image encryption using crossover operator and chaos,” Multimedia Tools and Applications, Vol. 75 No. 8:pp. 4753-4769, 2016.
[30] X. Wang, C. Liu, D, C. Liu, “Image encryption scheme using chaos and simulated annealing algorithm,”.Nonlinear Dynamics, Vol. 84, No. 3, 2016.