Ultra-key Space Domain for Image Encryption using Chaos-based Approach with DNA Sequence

Ibrahim AlBidewi[1]
Department of Information System,
Faculty of Computing and Information Technology
King Abdulaziz University, Jeddah, Saudi Arabia

Nashwan Alromema[2]
Department of Computer Science
Faculty of Computing and Information Technology-Rabigh
King Abdulaziz University, Rabigh, Saudi Arabia

***Abstract*—Recently, image encryption has taken an importance especially after the dramatic evolution of the internet and network communication. The importance of securing the images contents is due to the simplicity of capturing and transferring of digital images in various communication media. Although there are many approaches for image encryptions, chaos-based image encryption approach is considered one of the most appropriate approaches because of its simplicity, security, and sensitivity to the input parameter. This research paper presents a new technique for encrypting RGB image components using nonlinear chaotic function and DNA sequence. A new image with the same dimensions of the plain-image is used as a key for confusions and diffusion process for each RGB components of plain-image. Experimental results show the efficiency of the proposed technique, simplicity, and high level of resistant against several cryptanalyst.**

***Keywords*—Chaos-based; image encryption; confusion; diffusion; color image; RGB components; DNA sequence**

I. INTRODUCTION

Images are the most common and popular multimedia data type now a days, due to the simple and easy way of capturing and transmitting [1]. The demand to transfer these images in a secure manner has also increased, and encryption is the preferred method to securely transfer image data. In addition, there are several drawbacks and weakness such as the requirement for powerful computing system and highly computational time, thus the implementation of these techniques cause low level of efficiency and it cannot guarantee data confidentiality and security [2]. Encrypting images that are sent over various communications channels has become one of the most important processes of most of the current applications and fields, such as military, educational, medical, industrial and social media [3], [4]. Image encryption can be defined as the use of set of process called algorithm to convert the plain image into a ciphered image in such a way that no one can recover it except for the sender and the intended recipient [2] [5]. A numerous image encryption techniques have been proposed, one of the most efficient techniques is the Chaos-based encryption [6]. Chaos-based encryption methods first introduced by Fridrich [7], [8], these methods are popular due to their randomness, unpredictability, sensitivity and topological transitivity. Fridrich suggested two processes for chaos-based image encryption: confusion and diffusion. The most important stages in image encryption is confusion which is considered about pixels position in plain image. Many efforts tried to kill the pixels neighbors' dependence by exchange the positions under certain condition to maintain the correlation of the pixels and the predictive of new pixels position [9]. We list in this section some of the related works starting with Choi et al. who proposed a framework by the using addition, rotation and XOR to achieve confusion and diffusion for the plain image. In the proposed framework the confusion-diffusion process is done by implement the rotation and XOR operation with chaotic sequences which are generated by the using of two logistic maps [10]. Another study by Bashir et al. proposed image encryption framework, this framework a 4-D chaotic image encryption technique based on a mechanism of dynamic state variables to increase the security and effectiveness of the chaos-based image encryption methods [11]. Kulsoom et al. proposed algorithm that is based on stream cryptography and it use DNA complementary rules in addition to one dimensional chaotic maps [12]. Kar et al. proposed bit-plane image encryption method chaotic, cubic, and quadratic maps. The proposed method is based on permutation, diffusion, and pixel randomization process, at first the proposed method generates chaotic two sequences by the using of the quadratic and the cubic map, then the generated two sequences will be used to shuffle the plain image. the shuffled image will decomposed into its bit-plain components to be encrypted later by the using of confusion and diffusion process [13]. Gu et al. proposed encryption algorithm for JPEG2000 images. The method suggested the use of bitwise XOR and cyclic rotation operation for 2-byte block encryption process also the repeating of encryption process is adopted to avoid an unwanted encryption marker code. The repeating of encryption process can neglect unnecessary computations [14]. Enayatifar et al. proposed a method for image encryption that is based on chaotic map and deoxyribonucleic acid (DNA). The process is started by convert two dimensional plain image into one dimensional array, then the process of pixel permutation is implemented by the using of chaotic map and deoxyribonucleic acid (DNA) while the diffusion is implemented by the using of DNA sequence and DNA operator both of permutation and diffusion of image pixels are done at the same time to reduce the sending time [15]. The remaining part of this article is structured as it follows: Section 2 introduces the background of image cryptography;

This project was funded by the Deanship of Scientific Research (DSR) under grant no. G- 526-611-1431.

The authors, therefore, acknowledge with thanks to DSR's technical and financial support representations Methodology

Section 3 introduces the proposed image encryption scheme with the key space. Section 4 describes the experimental results. Section 5 introduces the security resistance and the ultra key space of the proposed encryption scheme. Lastly, Section 6 draws the conclusion and future work.

II. Image Cryptography

Image encryption like the encryption of any other kind of digital data, it goes through the encryption process using specific encryption algorithm and a key [1]. Steganography is one of the encryptions methods that have been used in image cryptography in the last two (2) decades and in particular on watermarking [16]. The classical image encryption such as Data Encryption Standard (DES), RSA, and ADS are designed with good confusion and diffusion [17], but it has the weakness of low-level of efficiency because of the huge size and noticeable redundancy of image data [3],[18]. Due to the big size of image data, the implementation of images cryptosystems is carried out in spatial domain, frequency domain or hybrid domains of the plain images. Each of these domains has its own methodology. For example, in spatial domain, the pixel value and location in plain image can be directly encrypted using the general encryption function as shown in Equation 1.

$$E(x,y) = f[I(x,y)] \quad (1)$$

Where $E(x,y)$ is the output encrypted pixel C_i in the ciphered image, $I(x,y)$ is the input plain pixel P_i in the plain image, and f is the encryption function. In frequency domain, image is analyzed mathematically to series of frequencies, each of these frequencies has two main components which are the amplitude and the phase shift [1]. Any changes in spatial domain image produce indirect change on its frequency domain representation. The information of frequency domain divided into two main components, and these components are high frequency components which represent sharp edges and noise of the plain image while the low frequency component corresponds to the smooth area [1]. In our proposed encryption scheme, we concentrate on spatial domain, frequency domain is out of the scope of our work. Classical and modern ciphers algorithms have all been developed for the simplest form of multimedia data. Chaos-based image encryption scheme is one of the encryption algorithms that works on spatial domain and that have suggested an efficient way to deal with fast and highly secure image encryption [18]. Encrypting images, using chaos-based image encryption scheme, considers the image as 2-dimensional array of pixels [5].

III. Proposed Image Encryption Scheme

The proposed image encryption algorithm in this research work is based on chaos-based image encryption scheme that has been proposed first by Fridrich [7], [8]. The scheme of the chaos-based image encryption is depicted in Fig. 1, as it is shown in Fig. 1 the plain image goes through two processes, namely, confusion process and diffusion process. At each stage there is a key input which is a single value starts with a seed value (easy to be predicted by cryptanalyst) and from this value the confusion key and key diffusion are created. In contrast, our proposed scheme follows Fridrich's scheme except the chosen key, in our proposed scheme the key is considered as another image (or on another say, a matrix of random values) with the same dimension (or bigger) the plain image.

The operations needed in encryption processes are confusion and diffusions as in. Both confusion and diffusion processes will be executed only one time for the purpose of reducing the computational time with the grantee of high level of security. Fig. 2 shows the general framework diagram of the proposed chaotic encryption algorithm. Stage (1), the plain-image and key image are gone through preparation process. The preparation process is responsible for analyse the chosen plain image and key image before passing them to the confusion process. The first check will be the size of plain image and key image, the key image should be equal or greater than the plain image, otherwise the process will fail. The second check will look for the plain image and key image, if they are in 8-bit grayscale the process will run and will deal with the images directly, while in 24-bits RGB images a new mechanism to extract the images (plain and key) RGB channels should be implemented to deal with each channel separately.

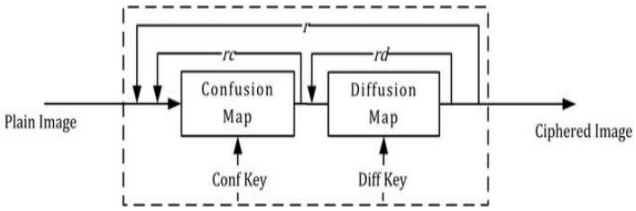

Fig. 1. Fridrich Image Encryption Scheme [8].

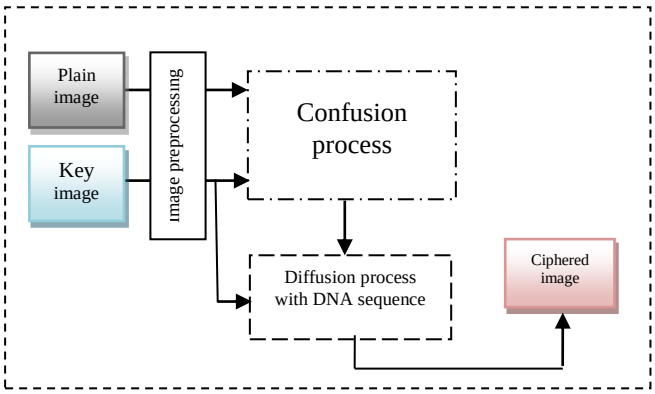

Fig. 2. Proposed Framework of Image Encryption Scheme.

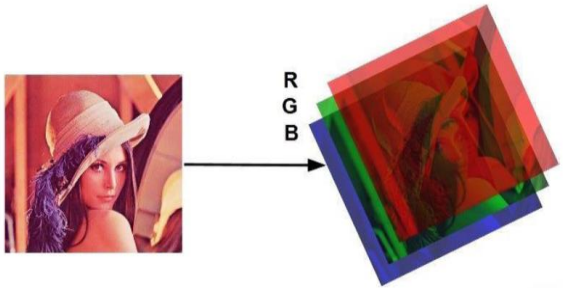

Fig. 3. 24-bit RGB Image Channels Extractions.

The extraction of the RGB channels of the plain and key images will store each image channel in a single 8-bits matrix with dimension equal to the dimension of the original image. Fig. 3 illustrate the extraction process that produces three channels image for plain and key image and each of these channels is 8-bit image. In the next subsections each process will be explained in detail.

A. Confusion Process

Confusion process goes through two processes, the RGB channels extraction (of both the plain image and the key image) and the confusion function that will be applied to each corresponding pixel in plain and key image as shown in Fig. 4. In confusion process, firstly, the chosen key image should be larger or of the same size of the plain image. Secondly, the confusion function which can be defined as any arithmetic, geometric, or bitwise function that will be performed on the corresponding pixels in RGB channels of the plain and key image as shown in Fig. 4. The chosen function should be strictly monotonically function (reversible function) [19], i.e., the encrypted pixel can be recovered back in the decryption process. For clarity, let RGB channels of the plain image represented by P_R, P_G, and P_B respectively. And for the key image, the RGB channels represented by K_R, K_G, and K_B respectively. For a plain image and key image with $n\ x\ m$ dimension, there are $n\ x\ m$ pixels, for simplicity we assume $n = m$, therefore number of pixels are n^2. In the confusion process, as explained previously, the corresponding pixels in plain and key images are operated by the confusion function (f) and result (an intermediate) new RGB channels with the same dimension of the original plain image.

Let us name these new channels as C_R, C_G, and C_B. The equations 2, 3, and 4 illustrate the operations for getting these channels (ciphered RGB), such that i and j are the indexes of the pixels and it ranges form $0 < i < n$ and $0 < j < n$. The function (f) is considered a bitwise XOR binary function in this study.

$$C_R(i,j) = f(P_R(i,j), K_R(i,j)) \quad (2)$$

$$C_G(i,j) = f(P_G(i,j), K_G(i,j)) \quad (3)$$

$$C_B(i,j) = f(P_B(i,j), K_B(i,j)) \quad (4)$$

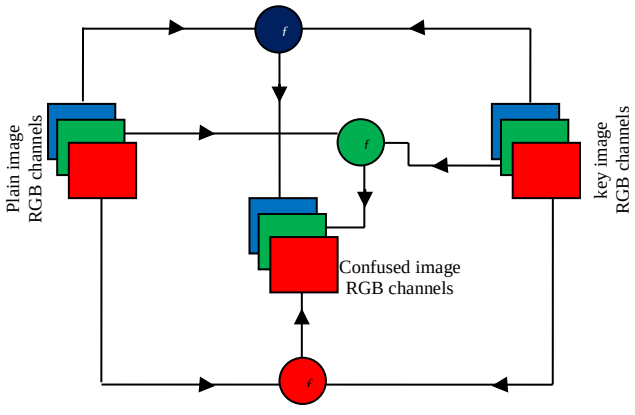

Fig. 4. Confusion Process for 24-Bit RGB Channels.

Confusion process is responsible for reducing the correlation between adjacent pixels by dissolving the pixels [9]. The method for dissolve this correlation is by applying confusion function of pixels in plain image and key image [3]. The output of this process is the RGB channels that will be input into the diffusion process.

B. Diffusion Process with DNA Sequence

Diffusion process starts at the end of confusion process and the output of confusion process will be the input of diffusion process. In this operation the output of confusion process will be encoded using DNA sequence computing as it will be explained in this section. DNA computing becomes important in many fields of research in the last four decades, in this research paper we employ DNA computing for the diffusion process. DNA sequence can be encoded and stored as a binary code of four pairs of two bits. The four chemical bases Adenine, Cytosine, Guanine, and Thymine are pair up with each other, A with T and C with G, each base-pair are the complement of each other. If we assume the binary coding of A is 00 therefore the binary coding of T is 11, and if the binary coding of C is 01 therefore the binary coding of G is 10. Therefore, for each pixel in the RGB channels (which come from confusion process) a new coding can be applied, for example, the pixel with binary 00101101 can be encoded using DNA sequence as AGTC as done in some related works [17], [20], [21]. The key image also will be encoded using the DNA sequence. The RGB channels which are the output of the confusion process will be operated with the RGB channels of the original key image using the logical addition and subtraction of the chemical bases as shown in Table I. The logical addition in this research work is employed for encryption process, the reverse operation which is the subtraction operation is employed in the decryption operation with the rules shown in in Table II.

As shown in Table II below the subtraction operation is reverse function of the addition function, therefore using one logical operation for encryption process enforces us to use the other operation for decryption.

TABLE I. DNA LOGICAL ADDITION OPERATION

+	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

TABLE II. DNA LOGICAL SUBTRACTION OPERATION

-	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

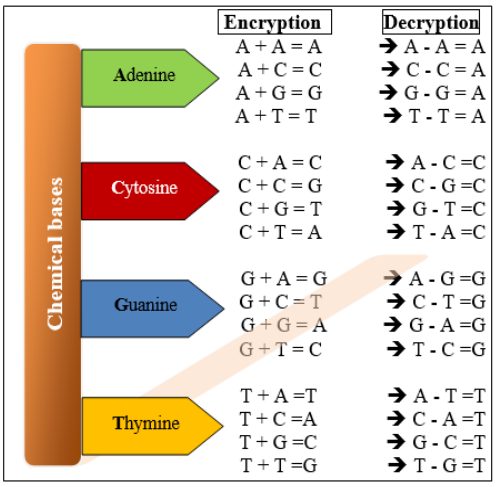

Fig. 5. The Encryption and Decryption of the Chemical bases **A**denine, **C**ytosine, **G**uanine, and **T**hymine using Logical Addtion and Subtraction Operations.

he four chemical bases for DNA sequence that are using in the diffusion are operated using logical addition for encryption and logical subtraction for decryption. Fig. 5 depicts the 16 possible scenarios for additions and the 16 possible scenarios for subtractions [15].

Finally, the Encryption and Decryption techniques are reverse to each other, therefore the last operation in encryption will be the first operation in decryption.

IV. Result Analysis

In this section, the detailed results to verify the efficiency, robustness, and high level of security of the proposed encryption scheme are outlined. A standard Lena image with 256 x 256 gray scale and a key image of the same size was used to verify the proposed methods performance as shown in Fig. 6. The experiment has been performed using visual studio package and implemented in windows environment. The first step the key image in Fig. 6(b) is prepared using the same proposed encryption scheme, second step2, the prepared key image together with the plain image (Lena image) in Fig. 6(a) are input to the encryption process, the result ciphered image is shown in Fig. 6(c). The Lena image is loaded to the encryption software, the key image is prepared using the same encryption algorithm to add more noise to the key image (any image can be used as a key without encrypt it) and to improve the encryption of the original image and the pixels distributions of the encrypted image that returns noisy images as shown in Fig. 6(c). These aspects indicate high level of security against the attacks.

The second experiment has been performed for Firise's image (293x203) as shown in Fig. 7. The chosen encrypted key image is in the same dimension (293x203) as the plain image. The same experiment with this image is performed in the previous studies with the contradiction that in our study we have less computation time and high performance. The same process for encrypting Lena image is applied for Firise image, whereas Fig. 7(a) represent the plain image, Fig. 7(b) represents the encrypted key-image, and Fig. 7(c) represents the encrypted (ciphered) image.

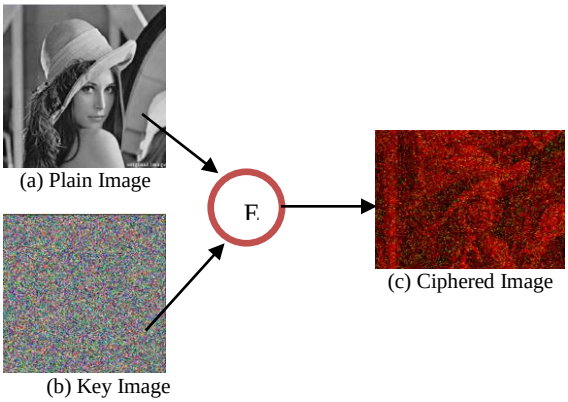

Fig. 6. Encryption Process for Lena Image (225x227), (a) Plian Image, (b) key Image, (c) the Encrypted Image.

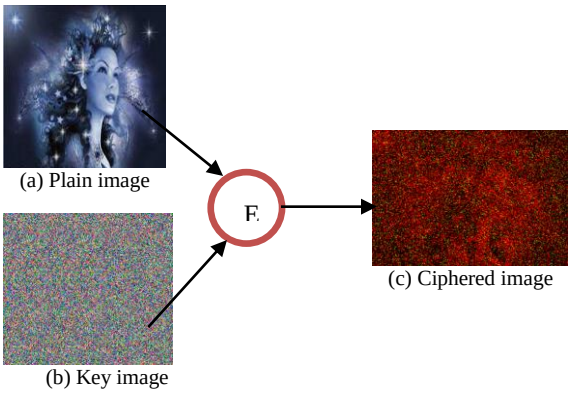

Fig. 7. Encryption Process for Firise Image (293x203), (a) Plian Image, (b) Key Image, (c) the Encrypteds Image.

The same methodology for image encryption using chaos-based approach has been conducted in our previous work [3]. Fig. 8 shows some of the experiments for encryption and decryption process for Lena image with 225x227 gray scale. The encryption process shown in Fig. 8 follows the same approach for conducting the proposed encryption scheme.

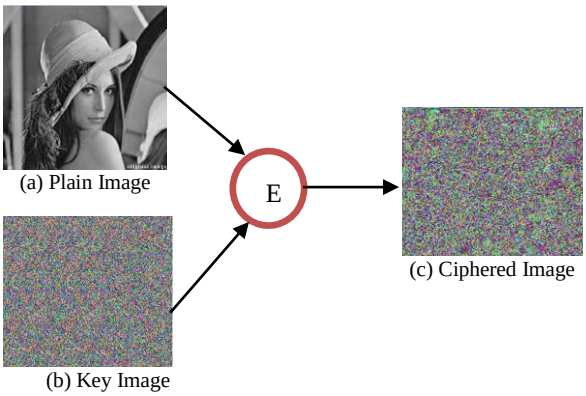

Fig. 8. Chaos-based Image Encryption Scheme[3], (a) Plian Image, (b) Key Image, (c) the Encrypted Image.

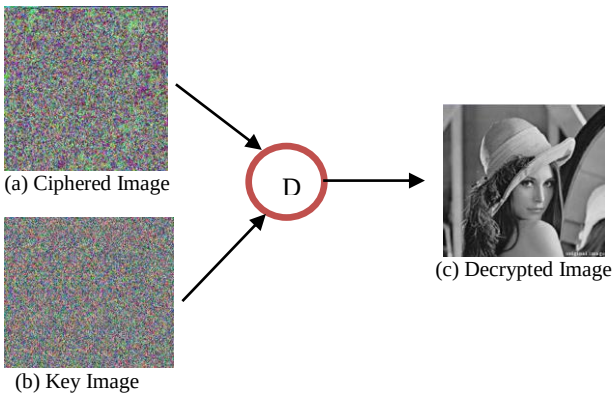

Fig. 9. Chaos-based Image Decryption Scheme [3], Lena Image (225x227), (a) Ciphered Image, (b) Key Image, (c) the Decrypted Image.

The reverse operation for image encryption is the decryption process. Fig. 9 shows the decrypted Lena image using the correct key image. Choosing wrong key image will not produce the correct plain image. For the key sensitivity and security analysis, next section investigates these issues.

V. Security Analysis

The proposed chaos-based image encryption scheme with DNA sequence coding has satisfied high-level of security, robustness, and efficiency, these features due to the high domain space of the key as well as the chaos features [22]. In this research work as well as our previous work, in [3], we use a key as an image for the encryption/decryption process in order to prevent the encrypted image against brute-force attack, statistical attack, known-plaintext attack and select plain text attack, these attacks are well known attacks listed in [3]. In the proposed cryptosystem, a confusion process is run, and the output goes to the diffusion process. If we assume we have $M \times N$-sized plain image, for simplicity put $M = N$ therefore the plain image will be N^2-sized image. For the encryption and based on the methodology of our encryption scheme the same key image dimension should be utilized i.e., we will need N^2-sized key image. Since the encryption process is working in bitwise therefore for gray scale image with 8 bits in each pixel, we will have $8*N^2$-sized key image with binary values 0 and 1. The possible combinations of a matrixes with $8*N^2$ binary values are in the domain 2^{8*N^2}, which increase exponentially as N increases. For the RGB channels the key space became ultra, since we will have 3 matrixes for R channel, G channel, and B channel, respectively and the key space become in $2^{8*N^2} * 2^{8*N^2} * 2^{8*N^2} = 2^{24*N^2}$. For example, a plain image of size 225x227 gray scale and key image with the same size, the brute-force attack needs to search the key in $2^{8*225*227} ==> 2^{51525}$ which is a very (ultra) large key space domain. This is the key point of our proposed algorithm, impossible for the key image to be predicated.

VI. Conclusion

The proposed study shows that the achieving of ideal secrecy system in cryptography can be performed with existence of confusion and diffusion processes. Despite the differential analysis is very interested attack but the proposed framework resolves this issue by the proposing of new technique for choosing key method. In general the proposed encryption framework consists of two processes (confusion and diffusion with DNA sequence) and one round of the two operations is grantee to produce high level of image security instead of having (n) rounds for confusion and (m) round in diffusion as in the conventional image encryption frameworks [7], [17], [23], [24]. This feature will reduce the computational time and the system complexity. The proposed confusion process (using confusion function) is responsible on the breach of high correlations of the adjacent pixels, while the diffusion process with DNA sequence logical operations increases withstanding against attack. Comparing to the several studies in literature our proposed algorithm's distinguished in terms of choosing the key as an image (instead of having single value) that contribute to high level of resistance of all kinds of attacks due to ultra-key space domain which is in the range of 2^{8*N^2} in the gray scale domain and 2^{24*N^2} in the RGB channels.

Acknowledgment

This project was funded by the Deanship of Scientific Research (DSR) under grant no. G- 526-611-1431. The authors, therefore, acknowledge with thanks to DSR's technical and financial support.

References

[1] H. Borrebach, "IMAGE ENCRYPTION FRAMEWORK BASED ON MULTI-CHAOTIC MAPS AND EQUAL PIXEL VALUES QUANTIZATION," no. Fb 14, p. 2018, 2018.

[2] M. Salleh, S. Ibrahim, and I. F. Isnin, "IMAGE ENCRYPTION ALGORITHM BASED ON CHAOTIC MAPPING The requirements of information security within an organization have undergone tremendous changes . Before the widespread use of data processing equi pment , the security of sensitive documents depends o," Image (Rochester, N.Y.), vol. 39, no. D, pp. 1–12, 2003.

[3] N. A. Al-Romema, A. S. Mashat, and I. AlBidewi, "New Chaos-Based Image Encryption Scheme for RGB Components of Color Image," Comput. Sci. Eng., 2012, doi: 10.5923/j.computer.20120205.06.

[4] M. SaberiKamarposhti, I. AlBedawi, and D. Mohamad, "A new hybrid method for image encryption using DNA sequence and chaotic logistic map," Aust. J. Basic Appl. Sci., vol. 6, no. 3, pp. 371–380, 2012.

[5] J. B. . Choudhary, R., &Arun, "Secure Image Transmission and Evaluation of Image Encryption.," Int. J. Innov. Sci. Eng. Technol., 2014.

[6] "Jain, A, Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform.," J. Netw. Commun. Emerg. Technol., vol. 6, no. 5, pp. 8–11, 2016.

[7] J. Fridrich, "Image encryption based on chaotic maps," Proc. IEEE Int. Conf. Syst. Man Cybern., vol. 2, pp. 1105–1110, 1997, doi: 10.1109/icsmc.1997.638097.

[8] M. Farajallah, S. El Assad, and O. Deforges, "Fast and Secure Chaos-Based Cryptosystem for Images," Int. J. Bifurc. Chaos, vol. 26, no. 2, 2016, doi: 10.1142/S0218127416500218.

[9] V. R. Divya, V. V., Sudha, S. K., &Resmy, "Simple and Secure Image Encryption.," Int. J. Comput. Sci. Issues., vol. 9, no. 3, pp. 286–289, 2012.

[10] H. Choi, J., Seok, S., Seo, H., & Kim, "A Fast ARX Model-based Image Encryption Scheme.," Multimed. Tools Appl., vol. 75, no. 22, pp. 14685–14706.

[11] S. Bashir, Z., Rashid, T., & Zafar, "Hyperchaotic Dynamical System based Image Encryption Scheme with Time-Varying Delays.," Pacific Sci. Rev. A Nat. Sci. Eng., 2016.

[12] S. A. (2016) Kulsoom, A., Xiao, D., & Abbas, "An Efficient and Noise Resistive Selective Image Encryption Scheme for Gray Images based on

Chaotic Maps and DNA Complementary Rules," Multimed. Tools Appl., vol. 75, no. 1, pp. 1–23, 2016.

[13] N. Nasser, M. Anan, M. F. C. Awad, H. Bin-Abbas, and L. Karim, "An expert crowd monitoring and management framework for Hajj," 2017, doi: 10.1109/WINCOM.2017.8238202.

[14] Z. Gu, G., Ling, J., Xie, G., & Li, "A Chaotic-cipher-based Packet Body Encryption Algorithm for JPEG2000 Images.," Signal Process. Image Commun., vol. 40, pp. 52–64, 2016.

[15] M. Enayatifar, R., Abdullah, A. H., Isnin, I. F., Altameem, A., & Lee, "Image Encryption using a Synchronous Permutation-Diffusion Technique," Opt. Lasers Eng., vol. 90, pp. 146–154, 2017.

[16] S. Nagaraj, G. S. V. P. Raju, and K. Koteswara Rao, "Image encryption using elliptic curve cryptograhy and matrix," in Procedia Computer Science, 2015, vol. 48, no. C, doi: 10.1016/j.procs.2015.04.182.

[17] S. Xu, Y. Wang, J. Wang, and Y. Guo, "A fast image encryption scheme based on a nonlinear chaotic map," ICSPS 2010 - Proc. 2010 2nd Int. Conf. Signal Process. Syst., vol. 2, pp. 1–16, 2010, doi: 10.1109/ICSPS.2010.5555472.

[18] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos, Solitons and Fractals, vol. 29, no. 2, pp. 393–399, 2006, doi: 10.1016/j.chaos.2005.08.110.

[19] E. Seeram, "Digital image processing.," Radiol. Technol., vol. 75, no. 6, 2004, doi: 10.4324/9781315693125-12.

[20] M. SaberiKamarposhti, I. AlBedawi, and D. Mohamad, "A new algorithm for image encryption using DNA sequence and cycling chaos," Aust. J. Basic Appl. Sci., vol. 6, no. 3, pp. 381–392, 2012.

[21] K. Singh and K. Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it," Int. J. Comput. Appl., vol. 23, no. 6, pp. 17–24, 2011, doi: 10.5120/2892-3779.

[22] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," Phys. A Stat. Mech. its Appl., vol. 351, no. 2–4, 2005, doi: 10.1016/j.physa.2005.01.001.

[23] X. Liu and A. M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," Proc. Second IASTED Int. Conf. Commun. Internet, Inf. Technol., pp. 527–533, 2003.

[24] L. Kocarev, "Chaos-based cryptography: A brief overview," IEEE Circuits Syst. Mag., vol. 1, no. 3, pp. 6–21, 2001, doi: 10.1109/7384.963463.