International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Diffusion Model Based on the Features of the 3D Chaotic Baker Map for Image Encryption

Akshay Chamoli[1], Jawed Ahmed[2], Mohammad Afshar Alam[3], Bhavya Alankar[4]

Submitted: 29/01/2023 **Accepted:** 04/04/2023

Abstract: This paper consists of an optimal encryption method for colored images with the technique of the 3D Chaotic Baker map-based diffusion model. The 2D Baker map introduced earlier was not secure against statistical attack and the performance was slow while encrypting an image. So, because the 2D Baker map did not show better results that are the reason 3D Baker Map came into existence and to merge the pixels to such an extent with each other so a little change in one bit of an original image can cause a whole lot of modification for the cipher. In the confusion method, it is functional to deal with the position of the pixels present within a specific image. The advantage of using the 3D Baker Map-based diffusion model in this paper as it makes the model delicate in nature for changing any pixel value or secret key. The algorithm's efficiency is dependent on the experimental results. The new proposed model for encryption with the inbuilt feature of random binary sequence for the process of encrypting the plain image to cipher.

Keywords: *2D Baker map, 3D Baker map, encryption, NPCR, UACI, and Diffusion.*

1. Introduction

The approach of encryption for image or video has its very own characteristic and requirement due to diverse homes of snapshots together with exclusive styles of facts their size and redundancy. The antique encryption methods consisting of DES, IDEA, Blowfish RSA, and AES are not green for image encryption and the purpose is their slow processing pace in the actual time environment and additionally, a large number of facts and correlation among the adjacent pixels and due to this most effective vintage cryptosystem strategies aren't green for picture encryption technique [1]. In terms of security, an expansion of algorithms was proposed in the past for picture encryption [2 - 4]. The results shown as chaos-based algorithms have various blessings in applications of bulk statistics encryption and it makes use of the vital houses of pseudo-randomness, ergodicity, and high sensitivity to number one situations and parameters is identified in showing the notable capacity for multimedia encryption because such features are considered analogous to those of vintage cryptosystem [5 - 6]. Sensitivity then again to initial situations simplifies that because the chaotic map is iteratively implemented to 2 extraordinarily close preliminary points, that iterates fast diverge, and turns out to be uncorrelated within the long term [7]. This function is helpful in photograph encryption as their adjacent pixels in a photo are extraordinarily correlated but when using a chaotic map, they will be uncorrelated after many rounds of the new release. The function of sensitivity with appreciation to parameters reasons the map to alter quickly at the same time as a bit the parameters on which the map dependency is present. The properties of the parameters considered are similar to a cipher key and in the case of encryption process enabled with chaotic-based features. Combining it with the tendency of the device to unexpectedly stability the little quantities of the kingdom space into an elaborate network of filaments. This character can scatter all of the correlated statistics over the phase space and those features bind up inside the formation of creating chaotic data encryption.

A lot of researchers proposed various kinds of chaotic methods with various dimensions. In respect of the division of dimensions, the chaotic method can be easily categorized into one and high-dimensional systems. Multiple variables are present for high-dimensional chaotic methods [8-9]. The chaotic orbits are unpredictable due to the feature of their highly complex situation and optimal chaotic characteristics. Some of the disadvantages of high dimensional chaotic systems are large computational costs as well as difficulty in realization. In comparison with high dimensional chaotic methods, the 1D chaotic methods use to have a simple design as well as they are easy to implement. The disadvantages as they have a very less chaotic range and are very vulnerable to attacks [10]. Some of the new research has been proven for cascade chaotic system [11], non-linear combination with the chaotic system, time

1Research Scholar, Department of Computer Science Engineering, Jamia Hamdard University, New Delhi, India-110062.
2,4Assistant Professor, Department of Computer Science Engineering, Jamia Hamdard University, New Delhi, India-110062.
3Vice-Chancellor, Jamia Hamdard University, New Delhi, India-110062.
Corresponding Author E-mail id: akachamoli@gmail.com

parameter control for chaotic system [12 -14], merging of DNA and chaotic system [15 - 17], and various others. In our research paper, a logistic map in a combination of the 3D baker map-based diffusion model has been used. The logistic map works on time parameters for controlling the state as well as parameters of chaotic methods. The other 3D Baker map-based diffusion model works on the logic to change the position of the pixel value, for example, if one bit is changed for the original image a vigorous amount of change happened in terms of pixels for the image cipher and vice versa. The improved chaotic map method has to shuffle and mix supported features. The security analysis factors it has given better results for the proposed model and are resistive against many types of attacks. Chaotic systems are of great interest to researchers for image encryption while some of the features of chaotic systems are sensitive to initial values, unpredictability, and randomness [3, 10, 13, 16, 21].

2. Related work

In literature, plenty has been carried out on the one-of-a-type algorithms which are primarily using the features of baker map. The Baker map is one of the unique features of 1D chaotic maps and helps in providing randomness with the help of generating fixed as well as sequenced pseudo-complexity random numbers that helps in reducing the complexity and providing better results. Han et. al [18] shared a permutation-based algorithm with the Baker map efficiency increased for more data to get encrypted at the same time. Different rounds of iterations are proposed using extraordinary cipher key consequences in a full-size type of ciphering key area. The encrypted statistics play a valuable feature in picture processing applications mainly at some stage in transmission. For speedy and relaxed photo encryption, chaotic maps are carried out to enhance picture encryption efficiency, and for system parameters, initial values have a huge key region. This paper delivered an easy set of guidelines for images encryption and decryption with the aid of way of using a chaotic Baker Map within the discrete Fourier rework (DFT). The proposed approach employs a baker map inside the frequency location to act on the transformed photograph coefficients which achieve excessive encryption overall performance. Shi et. Al [19], proposed an image encryption version based totally on the Baker map with the utility of a pseudo-random variety generator. Further, a unidirectional hybrid control approach is. In this paper, a unidirectional hybrid control technique is proposed to beautify the dynamic homes and cast off the biases of virtual chaotic maps. Csernaket. Al [20] proposed a two - dimensional micro-chaos map, a multi-baker map that incorporates a finite series of baker's maps. Kuperinet. Al [21] proposed a -dimensional chaotic map, especially, the baker map. The technique is based on the probabilistic coupling of the managed dynamics with a controlling device and the subsequent lifting of the coupled dynamics to a suitable useful area. Elshamyet. Al [22] introduced a chaotic Baker map merging with Double Random Phase Encoding (DRPE) for cipher generation on optical images. This process involves layers to improve the safety degree of the classical DRPE. The initial layer present is a pre-processing layer, involving various images with a chaotic-based map, for the second layer, the standard DRPE is processed. Chen et.al [23] supplied a way wherein the proper machine employs a chaotic Baker map preceding DRPE to offer more protection to the plain picture and as an end result sell the protection level of DRPE, as claimed. However, cryptanalysis indicates that this scheme is susceptible to a delegated-plaintext assault, and the ciphertext can be exactly recovered. Liu et. Al [24] shared an encryption method based on optical process and is fully based on Baker mapping in 1D fractional Fourier domain. Wang et al. [25] shared sine maps and 1D chaotic maps to merge and prevent plaintext attacks. The paper sections are divided as follows: Section2 deals with the knowledge of advancement in logistic chaotic map. Section3 has explained the complexities and their performances, their parameters, and space. Section4 deals with the encryption methods for images. Section5 consists of the experimental results obtained and section6 has the overall conclusion of the paper.

3. Baker Map

The cryptographic model commonly has 1D chaotic map features because of its efficient behavior and easy structure. The 1D map has various features including both the initial and control parameter and due to these features, the encryption model sometimes behaves inappropriately [75]. The chaotic map is a larger version of the Bakers map providing the features of randomization with the motive of producing a unique amount of pseudo-random numbers which eventually will help in efficient cryptography.

Mathematically, Baker map (B) is defined as follows:

$$B(x,y,z)=\begin{cases}\left(2x,\,2y,\,\frac{z}{4}\right) & 0\le x<\frac{1}{2},\,0\le y<\frac{1}{2}\\ \left(2x,\,2y-1,\,\frac{z}{4}+\frac{1}{2}\right) & 0\le x<\frac{1}{2},\,\frac{1}{2}\le y\le 1\\ \left(2x-1,\,2y,\,\frac{z}{4}+\frac{1}{4}\right) & \frac{1}{2}\le x<1,\,0\le y<\frac{1}{2}\\ \left(2x-1,\,2y-1,\,\frac{z}{4}+\frac{3}{4}\right) & \frac{1}{2}\le x\le 1,\,\frac{1}{2}\le y\le 1\end{cases}$$

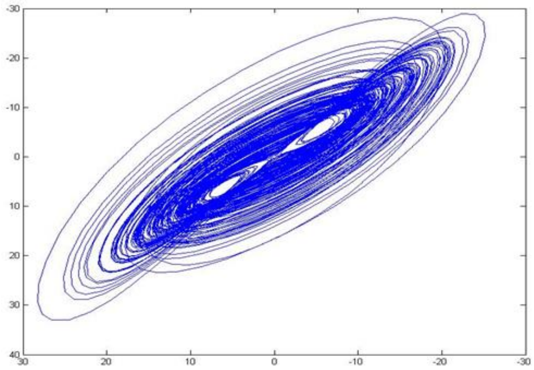


Fig (a)

3.1 Confusion method

A mathematical relation having complex features can be obtained among the secret key and ciphertext and is retrieved after the encryption method. In this, all the parts for the cipher are dependent on each other with respect to the original message and its subkeys. These results were obtained and able to survive the different types of attacks. The Baker logistic map generated key streams which are CK1, CK2, and CK3, and further moved down to (10), (11), and (12) to be used in the confusion process [3, 4]**.**

CK1 (i, j) =abs(CK1 (i,j) * 104 MOD 256**)** **(10)**

CK2 (i, j) =abs(CK2 (i,j) * 104 MOD 256**)** **(11)**

CK3 (i, j) =abs(CK3 (i,j) * 104 MOD 256**)** **(12)**

The CK1, CK2 and CK3 symbolize red, green and blue color channels.

3.2 Diffusion method

In an encryption set of rules the diffusion procedure is wherein pixels are sure together and cipher textual content is generated to be made touchy to alternate in plaintext [7] [9]. So it may be concluded that the diffusion process is vital to face up for the cryptographic process using differential method; a selected image pixel, and fully responsible on key flow as well as prior pixel values [42, 45]. Using the preliminary conditions x1, y1 and z1 (1), (2) and (3) iterate MN+1 thousand instances, and the primary first thousand values are neglected for temporary results. Further, chaotic sequences i.e. KD1, KD2 and KD3 are acquired using (13), (14) and (15).

Hence the diffusion manner is implemented among two adjoining pixels of a 3D Baker map. It is defined below.

KD1 (i, j) =abs(KD1 (i,j) * 104 MOD 256**)** **(13)**

KD2 (i, j) =abs(KD2 (i,j) * 104 MOD 256**)** **(14)**

KD3 (i, j) =abs(KD3 (i,j) * 104 MOD 256**)** **(15)**

KD$_1$, KD$_2$ KD symbolizes three colors namely red, green and blue.

Simulation results

Encryption scheme

The proposed model introduced in this paper follows few steps to conclude:

Step1: Production of key

Step2: Merging of random data

Step3: Prepossessing

Step4: shuffling

Step5: confusion and diffusion

The steps are useful in the modification of image features and finally provides the output

These all steps are accompanied to modify the picture functions and its responsibilities in the encrypted or cipher image. Information integration randomly with the nearby pixels of an image. The first step includes random numbers addition with pixels for a picture [22]. The next step involving change in pixel value with the process of shuffling and can be implemented towards various images. The notation 0 represents black color while 1 represent white color. The technique of shuffling reduces the character of correlation many of the close by pixels and at closing the diffusion model primarily based on 3-d Baker map is carried out.

The modified model based on cryptography is in Fig.4. The new encryption approach is shown as

Step 1: The color image represents in a 3 band channel.

Step 2: The method represented as Pseudo random generator having 280-bit long, unique key is obtained and is also used to produce an expansion of parameters for baker Map.

Step 3: For an image the randomly generated information is merged with the environment [71].

Step 4: The Brownian movement model is involved with analyzing every and each pixel intensity value and then modifying every channel for every pixel and XORing the key stream and is produced. .

Step 5: shuffling each channel with the assist of chaotic collection and is produced using logistic map.

Step 6: The 2D Baker Map method is applied for better end results among pixels [19].

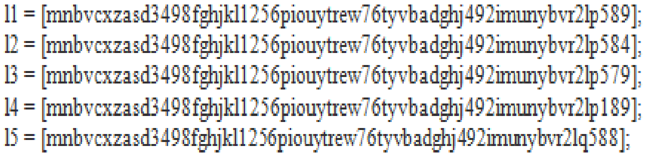
Step 7: Finally the 3-D Baker map based diffusion method is implemented, making sure propagation of change in a pixel to the maximum of the pixels. It shows the modification in almost every pixel present and even a change in a single pixel change the direction of cipher to an efficient quantity. Figure 5 has shown the two images title Lena and Pepper for the method of encryption and decryption of the given model [85].

Encryption and Decryption analysis

The analysis for encoding and decoding process shown in Fig. 8. In the paper four pics are taken for checking out encryption algorithm, “Lena”, “Horse”, “Cameraman”, and “Relief”, in which “Lena”, “Horse” and “Cameraman” are natural photographs, and “Relief” is a pc composite image. The simulation output shows that the cipher obtained can have noisy things so that any facts or records can't be retrieved. In case of decryption technique with the proper secret keys the images received might be retrieved equal because of the authentic images.

Key sensitivity

A cryptographic process is always the sensitive with respect to changing the secret key. If a 1- bit change is done in a key then the generation of a random cipher also generates l1, l2, l3, l4, l5 and these are also a one bit change keys.



```
l1 = [mnbvcxzasd3498fghjkl1256piouytrew76tyvbadghj492imunybvr2lp589];
l2 = [mnbvcxzasd3498fghjkl1256piouytrew76tyvbadghj492imunybvr2lp584];
l3 = [mnbvcxzasd3498fghjkl1256piouytrew76tyvbadghj492imunybvr2lp579];
l4 = [mnbvcxzasd3498fghjkl1256piouytrew76tyvbadghj492imunybvr2lp189];
l5 = [mnbvcxzasd3498fghjkl1256piouytrew76tyvbadghj492imunybvr2lq588];
```

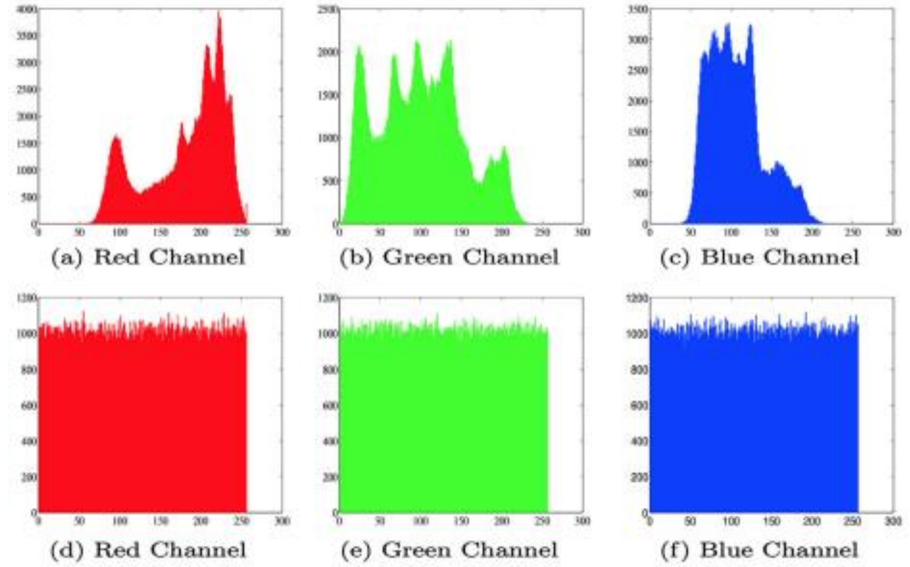
Key sensitivity shares

(i) Cipher is very dependent on the logic of one bit change in key to a massive change in the cipher. For a given plain image when encrypted having the functionality of two keys and for a one bit change having output images will be obtained completely different.

(ii) The encoded picture should not change back to its unique picture in regard of having a little alteration, similar to a little bit change in a secret key.

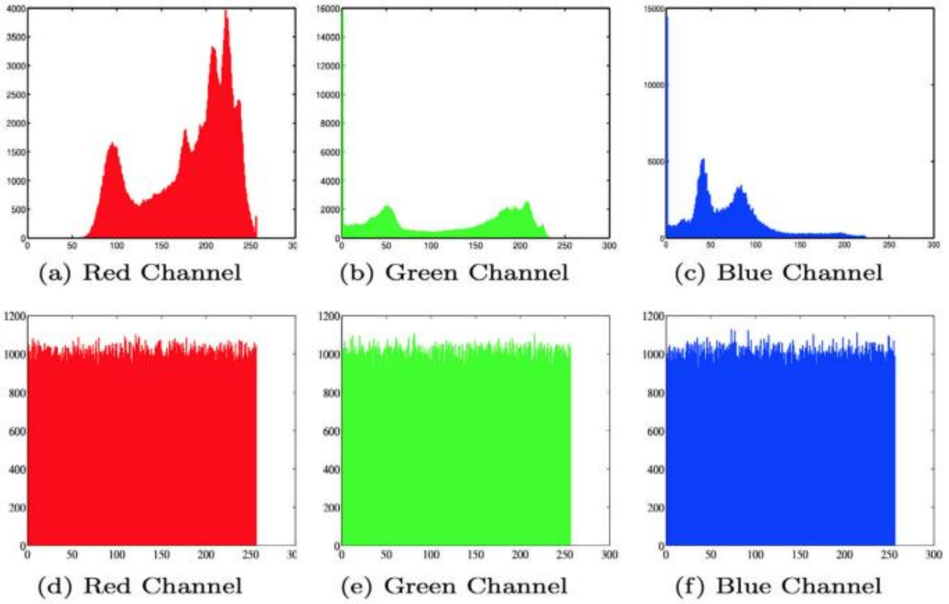
The analysis of Histogram

The Histogram provides the pixels distribution for an image in the form of a graph. For a better encryption process, the cipher images should have the property of uniform histogram so that it can easily resist any type of statistical attacks. Cipher and original images are depicted in in Fig. 9 and Fig. 10. The results shown as encrypted images are uniform in respect to plain or original images.


(a) Red Channel (b) Green Channel (c) Blue Channel

(d) Red Channel (e) Green Channel (f) Blue Channel

Fig. 9 Lena a-c and Cipher image d-f histogram


(a) Red Channel (b) Green Channel (c) Blue Channel

(d) Red Channel (e) Green Channel (f) Blue Channel

Fig. 10 Images with histogram

Correlation procedure

It depicts the two random variables and their linear relationship with respect to two nearby pixels in image processing. The plain images pixels should have maximum correlation to their adjacent pixels. The correlation among two nearby pixels should be very low so that the various directions namely horizontal, vertical, or diagonal can be analyzed smoothly.

Table 1: Correlation values for different images

Images	**Horizontal results**	**Vertical results**	**Diagonal results**
Lena image	0.9355	0.9544	0.9061
Lena cipher	0.000579	0.00062	-0.00031
Pepper image	0.9357	0.9549	0.9160

Pepper cipher	0.00089	- 0.00037	-0.00064
Ref.[26]	-0.028872	0.014593	0.036587
Ref.[27]	-0.0055002	0.0041189	0.0002136

Resistance to a variety attack and their analysis

The few parameters were examinedfor differential attacks, namely, wide variety of pixel exchange fee (NPCR) and unified average changing depth (UACI). To resist any kind of differential attack, the procedure must have excellent sensitivity to standard images, which means a minute change in original image will create a massive change in cipher image. NPCR and UACI may be calculated as:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{L} \times 100\%$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$\mathrm{UACI} = \frac{1}{L}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{H}\right] \times 100\%$$

C1 and C2 images having the same size, showing the original and cipher images, respectively. L is M × N, and price for H is 255 for color snap shots. For shade photographs, an appropriate fee of NPCR is 0.9961, and the appropriate fee of UACI is 0.3347.Anytime change of 1-bit in the original image and then gets encrypted as C2. While comparison among NPCR and UACI in the process towards our goal value, and it states that the proposed encryption method is optimal and efficient to resist various kinds of differential attacks.

Table 2: Comparison among NPCR and UACI for different models

Test	[Lozi Map]	[Lorenz Map]	[Chen map]	[Ref. 26]	[Ref. 27]	Proposed Map
NPCR%	99.60	99.61	99.59	99.60	99.61	99.62
UACI%	33.42	33.41	33.46	33.45	33.41	33.47

4. Conclusion

This paper having, 3D Baker map based diffusion model and logistic map technique is being used. The positive impact of 3D Baker map based on the diffusion model is under its control the original logistic map also becomes efficient. The parameters used under logistic map varying, and the logistic sequence being generated is non-stationary. The demerit of the logistic map which is blank and stable window size is improved. Statistical checks and protection analyses are the numerous take a look at effects which are depending on the overall results achieved from encryption algorithm which include numerous analysis factors along with histogram analysis, statistics entropy evaluation, key area analysis, key sensitivity evaluation, correlation evaluation, resistance to differential attack evaluation and robustness analysis and the effects proven that the changed three-D Baker map primarily based diffusion version had green chaotic capabilities and complexity. The various test results obtained for this paper including encryption algorithm model shows optimal security performance and large complexity. Due to these features only many types of attacks are resisted. The main feature of this paper is modified 3D Baker map and utilizing it as a diffusion model, implemented with map having an efficient encryption algorithm having optimal security as its main feature.

References

[1] Chai, X., Chen, Y., &Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA

sequence operations. *Optics and Lasers in engineering*, *88*, 197-213.

[2] Chen, H., Tanougast, C., Liu, Z., Blondel, W., &Hao, B. (2018). Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform. *Optics and Lasers in Engineering*, *107*, 62-70.

[3] Raghuvanshi, K. K., Kumar, S., & Kumar, S. (2020). A data encryption model based on intertwining logistic map. *Journal of Information Security and Applications*, *55*, 102622.

[4] Raghuvanshi, K. K., Kumar, S., Kumar, S., & Kumar, S. (2021). Development of a new encryption system using Brownian motion based diffusion. *Multimedia Tools and Applications*, *80*(14), 21011-21040.

[5] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, *8*(06), 1259-1284.

[6] Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6-21.

[7] Kumar, S., Kumar, R., Kumar, S., & Kumar, S. (2019). Cryptographic construction using coupled map lattice as a diffusion model to enhanced security. *Journal of Information Security and Applications*, *46*, 70-83.

[8] Hua, Z., Jin, F., Xu, B., & Huang, H. (2018). 2D Logistic-Sine-coupling map for image encryption. *Signal Processing*, *149*, 148-161.

[9] Tong, X., & Cui, M. (2009). Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. *Signal processing*, *89*(4), 480-491.

[10] Belazi, A., Abd El-Latif, A. A., &Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, *128*, 155-170.

[11] Lan, R., He, J., Wang, S., Gu, T., &Luo, X. (2018). Integrated chaotic systems for image encryption. *Signal Processing*, *147*, 133-145.

[12] Annaby, M. H., Rushdi, M. A., &Nehary, E. A. (2018). Color image encryption using random transforms, phase retrieval, chaotic maps, and diffusion. *Optics and Lasers in Engineering*, *103*, 9-23.

[13] Silva-García, V. M., Flores-Carapia, R., Rentería-Márquez, C., Luna-Benoso, B., &Aldape-Pérez, M. (2018). Substitution box generation using Chaos: An image encryption application. *Applied Mathematics and Computation*, *332*, 123-135.

[14] Sui, L., Lu, H., Wang, Z., & Sun, Q. (2014). Double-image encryption using discrete fractional random transform and logistic maps. *Optics and Lasers in Engineering*, *56*, 1-12.

[15] Akhavan, A., Samsudin, A., &Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. *Optics & Laser Technology*, *95*, 94-99.

[16] Dou, Y., Liu, X., Fan, H., & Li, M. (2017). Cryptanalysis of a DNA and chaos based image encryption algorithm. *Optik*, *145*, 456-464.

[17] Pujari, S. K., Bhattacharjee, G., &Bhoi, S. (2018). A hybridized model for image encryption through genetic algorithm and DNA sequence. *Procedia Computer Science*, *125*, 165-171.

[18] Han, F., Yu, X., & Han, S. (2006, January). Improved baker map for image encryption. In 2006 1st International Symposium on Systems and Control in Aerospace and Astronautics (pp. 4-pp). IEEE.

[19] Shi, Y., & Deng, Y. (2021). Hybrid control of digital Baker map with application to pseudo-random number generator. *Entropy*, *23*(5), 578.

[20] Csernák, G., Gyebrószki, G., &Stépán, G. (2016). Multi-baker map as a model of digital PD control. *International Journal of Bifurcation and Chaos*, *26*(02), 1650023.

[21] Kuperin, Y. A., &Pyatkin, D. A. (2005). Two-dimensional chaos: the baker map under control. *Journal of Mathematical Sciences*, *128*(2), 2798-2802.

[22] Elshamy, A. M., Rashed, A. N., Mohamed, A. E. N. A., Faragalla, O. S., Mu, Y., Alshebeili, S. A., &Abd El-Samie, F. E. (2013). Optical image encryption based on chaotic baker map and double random phase encoding. *Journal of Lightwave Technology*, *31*(15), 2533-2539.

[23] Chen, J. X., Zhu, Z. L., Fu, C., Zhang, L. B., & Zhang, Y. (2014). Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding. *Journal of Optics*, *16*(12), 125403.

[24] Liu, Z., Li, S., Liu, W., & Liu, S. (2013). Opto-digital image encryption by using Baker mapping and 1-D fractional Fourier transform. *Optics and Lasers in Engineering*, *51*(3), 224-229.

[25] Wang, H., Xiao, D., Chen, X., & Huang, H. (2018). Cryptanalysis and enhancements of image encryption using a combination of the 1D chaotic map. *Signal processing*, *144*, 444-452.

[26] Yavuz, E., Yazıcı, R., Kasapbaşı, M. C., &Yamaç, E. (2016). A chaos-based image encryption algorithm with simple logical functions. *Computers & Electrical Engineering*, *54*, 471-483.

[27] Song, C. Y., Qiao, Y. L., & Zhang, X. Z. (2013). An image encryption scheme based on new spatiotemporal chaos. *Optik-International Journal for Light and Electron Optics*, *124*(18), 3329-3334.