E-ISSN: 3048-6041 | Volume- 2, Issue- 3 | March 2025

A Study on Chaos-Based Image Encryption: Arnold Cat Map and Bogdanov Map in Action

Sonali Mahapatra[1], Mr. Ramakant Parida[2], Dr. Chittaranjan Pradhan[3]
[1]M.Tech. Student, Department of Computer Science, KIIT University, Bhubaneswar, Odisha.
[2]Assistant Professor, Department of Computer Science, KIIT University, Bhubaneswar, Odisha.
[3]Associate Professor, Department of Computer Science, KIIT University, Bhubaneswar, Odisha.

ABSTRACT:

Chaotic maps and cryptographic techniques are important for advancing digital image encryption methods. Digital images, consisting of pixels arranged in various dimensions, are often vulnerable to unauthorized access, tampering, or data extraction during transmission over networks or other media. To address these challenges, this research focuses on large-scale image encryption using Arnold Cat Map and Bogdanov map. These chaotic maps are evaluated for encryption and decryption processes in terms of metrics like time efficiency and computational complexity. Besides that, the security parameters of UACI (Unified Average Changing Intensity) and NPCR (Number of Pixels Change Rate) are tested to analyze the capability of the encryption methods to withstand differential attacks. The other criteria that have been taken into consideration include entropy and correlation coefficient, for the assessment of randomness, distribution, and the robustness of the encryption techniques against statistical and visual analysis attacks. The integration of chaotic maps with cryptographic strategies not only enhances the security of digital images but also ensures their efficient encryption and decryption processes. The diverse set of chaotic maps used in this study demonstrates flexibility in meeting different performance and security requirements. This comprehensive analysis highlights the potential of chaotic maps as robust tools for image encryption, paving the way for further advancements in secure digital communication and data protection.

Keywords: Chaotic map, Entropy, NPCR, UACI, Correlation Coefficient

INTRODUCTION:

With rapid advancements in networking and data communication, the volume of digital information transmitted through various media has grown exponentially. Images, as one of the most major and essential forms of data, are created and shared daily in vast quantities through means such as television, smartphones, personal computers, tablets, and satellites [1]. These technological developments have empowered users to design and manage image-based systems, yet they have also introduced significant challenges related to copyright protection and securing images against unauthorized access [2]. Advanced security techniques have been developed to address these challenges, and one of the most effective solutions has been image encryption. Image encryption protects the content by transforming an original image into an encrypted, unreadable form to unauthorized users from accessing its information [3]. High dependence on internet and improving data engineering demands more robust mechanisms for securing digital private or sensitive data [4]. While images and videos have their own specific attributes such as larger file sizes, pixel correlation, and the prevalence of applications on the

internet, it requires specialized protection mechanisms. Traditional cryptographic methods like DES, AES, and RSA have been proven to be suitable for text-based data, whereas they are not ideal for multimedia data due to high computational complexity and rigidity in accommodating image-specific features [5]. The systems utilize the intrinsic properties of chaos, such as sensitivity to initial conditions and pseudo-randomness, to provide greater security [6]. This will render the encrypted image totally unrecognizable to unauthorized users. Different methods of image encryption have been developed to prove ownership and secure image data [7]. Chaos-based methods have also gained considerable attention due to their unique features, such as extreme sensitivity to initial conditions and control parameters, pseudo-random behavior, and non-periodicity [8]. These features, coupled with the ease of implementation, make chaos-based encryption highly effective and adopted for securing digital images in large numbers [9]. Chaotic encryption performs multiple steps to hide the information from the image data. First, it scrambles the spatial pixel positions in a way to break the visual correlation among the pixels [10]. In so doing, it makes it impossible to distinguish the features of the original image completely. It decomposes an image into its binary plane to gain better control over the encryption process [11]. Different performance parameters are used to measure the effectiveness of chaos-based encryption techniques. Parameters such as NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are measured to ensure the sensitivity of the encryption method towards minute changes in the input image, thus resisting differential attacks efficiently [12]. Entropy analysis tests the randomness of the encrypted image, where a greater entropy value is related to higher resistance towards statistical attacks [13].

2.Preliminary

2.1. Arnold Cat Map:

The 2D Arnold cat map was found by Vladimir Arnold, is a pixel-shuffling algorithm that never stops changing the locations of the pixels in an image by visiting numerous iterations. With an increase in the number of iterations, the coordinates of the pixels in the square matrix become repetitive. This 2D Arnold cat map displays chaotic behaviour, but with better security and randomness than that of the 1D cat map. For an M x M image, the coordinates are taken as M (i, j) . It is defined as

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = A \begin{bmatrix} X \\ Y \end{bmatrix} \text{mod } 1 \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (1)$$

Where,

$$A = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$$

In this case, parameter x and parameter y are the controls of the system. By applying the transformation to original coordinates i and j of the pixel one will obtain new coordinates i' and j'. Old positions are substituted with the new ones for each cycle of the Arnold 2D cat map. By a few repeated iterations, the jumbled picture returns to its initial pixel arrangement whereby this is called the Arnold period. When combined with the diffusion, the process is also heard hence enhances security.

E-ISSN: 3048-6041 | Volume- 2, Issue- 3 | March 2025

2.2 Bogdanov Map:

The Bogdanov map forms the backbone of current image encryption schemes, especially those that use cellular automata. It modifies both pixel intensity values and spatial positions, ensuring a high level of randomness and obscurity in the encrypted images. The chaotic map helps form a cryptosystem that is impressively secure with respect to the key space, thus making it resistant to brute-force attacks. In addition, the inherent complexity of the Bogdanov map helps in the generation of complex encryption patterns, and the computational efficiency of the map allows for fast encoding and decoding processes. These features make it an effective tool for secure and high-performance image encryption.

$$x_{i+1} = x_i + y_{i+1} \quad (2)$$

$$y_{i+1} = y_i + a y_i + b\,(x_i - 1) + c\,x_i\,y_i$$

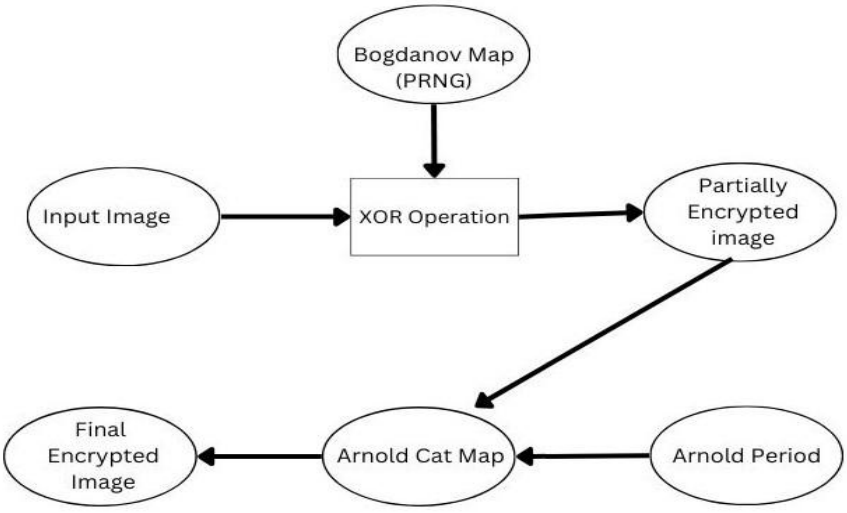
Where a, b, c are the control parameters.

This method works by rearranging the pixel positions in the original image through a scrambling process dictated by the Bogdanov map. A single key (b) is used for both the scrambling and descrambling processes, ensuring that the original image can be fully restored. The approach is versatile, allowing images of any size or dimension to be scrambled directly, without the need to divide them into smaller segments. This removes the constraint on the dimensions of the photograph. The original image is recovered at the end of a number of iterations, here equal to the period of the Bogdanov map, which is defined as the number of iterations until all pixels return to their original positions.

3. Proposed Methodology:

In this section, our proposed methodology will discuss under two heading i.e. proposed methodology for image Encryption and proposed methodology for image Decryption.

3.1: Proposed Methodology for Image Encryption:



[Fig:1 ENCRYPTION PROCESS]

Step:1 Input Image Processing

The original image serves as the primary input to the encryption system. The encryption process aims to transform this image into a highly unrecognizable and secure form.

Step:2 XOR-Based Partial Encryption

- A Pseudo-Random Number Generator (PRNG) based on the Bogdanov Map is used to generate a random sequence of values.
- This PRNG output is then applied to the input image using a bitwise XOR operation, which results in a partially encrypted image.
- The XOR operation introduces randomness and masks the pixel values, ensuring an initial layer of security.

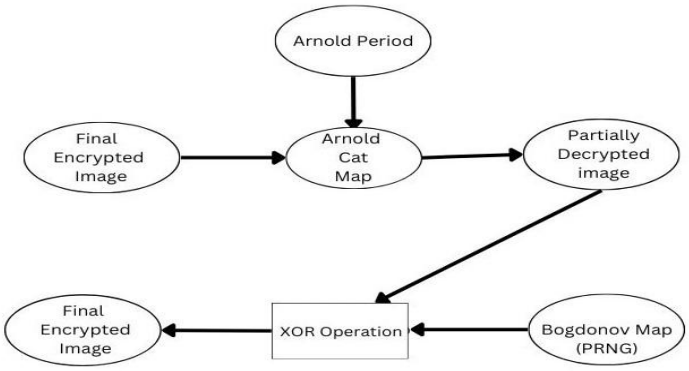
Step:3 Arnold Cat Map for Image Scrambling

- The partially encrypted image undergoes a transformation using the Arnold Cat Map (ACM), a chaotic permutation function.
- ACM redistributes the pixel positions based on a non-linear mapping function, increasing the complexity of the encryption.
- The Arnold Period defines the number of iterations required before the image returns to its original state. This period is crucial for determining the security strength of the transformation.

Step:4 Final Encrypted Image

- After a sufficient number of Arnold Cat Map iterations, the image becomes completely scrambled and unrecognizable.
- The resulting image is the final encrypted image, which ensures enhanced security against attacks and unauthorized access.

3.2: Proposed Methodology of Image Decryption Process:



Decryption Process

Step:1: Input - Final Encrypted Image

- The decryption process begins with the final encrypted image, which has undergone XOR-based substitution and Arnold Cat Map-based permutation during encryption.
- The goal is to reverse these transformations to recover the original image.

Step 2: Arnold Cat Map (ACM) Inversion

- The Arnold Cat Map (ACM) is applied in reverse using the same Arnold Period as in encryption.
- Since the Arnold Cat Map is periodic, applying it in reverse for the correct number of iterations restores the pixels to their original positions.
- This step **reverses** the scrambling effect, leading to a partially decrypted image, but the pixel values are still masked.

Step:3: XOR Decryption using Bogdanov Map (PRNG)

- The partially decrypted image undergoes an XOR operation with a pseudo-random sequence generated by the Bogdanov Map-based PRNG (Pseudo-Random Number Generator).
- Since XOR is a self-inverse operation, applying XOR again with the same PRNG sequence as in encryption restores the original pixel values.
- This step removes the randomness introduced during encryption, revealing the original image.

Step:4: Output - Original Image Recovery

- After performing XOR decryption, the original image is completely recovered.
- The final output is identical to the original input image, ensuring a successful and secure decryption process.

4.Analysis of Security:

4.1 NPCR and UACI:

Utilizing the chaotic characteristics of these maps, high sensitivity to initial conditions as well as control parameters may be achieved to the point that slight variations may result in drastic changes in outcomes. The effectiveness of encryption is evaluated by doing pixel-based analysis on the original and encrypted images, respectively, with particular regards to NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) as two evaluation metrics.

$$\text{NPCR} = \frac{\sum_{i,j} K(i,j)}{a*b} * 100\%$$

$$\text{UACI} = \frac{\sum_{i,j}\left\{\frac{|p(i,j)-Q(i,j)|}{255}\right\}}{a*b} * 100\%$$

It is preferred in digital image encryption to have higher values of NPCR because this measures or calculates the alterations in terms of pixels between a clear image and its encrypted version []. This criterion defines the functioning of an encryption algorithm, proving the encrypted image dissimilar from the original image. Besides NPCR, another important metric discovered to be very fundamental in evaluating average intensity differences between two images is UACI (Unified Average Changing Intensity). Collectively, these two metrics, NPCR and UACI, provide a robust framework for the strength and randomness evaluation of this encryption technique-very important for a critical image security analysis.

IMAGE	NPCR Values	UACI Values
Peppers64	99.5361	29.1941
Peppers128	99.6033	29.6779
Peppers256	99.6063	29.6958
Peppers512	99.6078	29.8352
Barbara64	99.5361	31.4800
Barbara128	99.5178	32.0577
Barbara256	99.6521	32.6358
Barbara512	99.6143	32.9925
Lena64	99.4629	28.1395
Lena128	99.6399	28.4096
Lena256	99.6735	28.8645
Lena512	99.6017	28.3633

Table:1: NPCR and UACI Values for Gray Scale Images

IMAGE	ENCRYPTION TIME(Sec)	DECRYPTION TIME(Sec)
Peppers64	0.7917	0.0071
Peppers128	2.7327	0.0148
Peppers256	7.7037	0.0517
Peppers512	47.01	0.2193
Barbara64	0.8588	0.0052
Barbara128	2.09	0.0142
Barbara256	13.03	0.0510
Barbara512	46.38	0.1865
Lena64	0.8254	0.0050
Lena128	2.9789	0.0148
Lena256	13.1020	0.0486
Lena512	42.7724	0.2125

Table:2 Encryption Time and Decryption Time in Sec of Gray Scale Images

4.2 Entropy:

The analysis of entropy information proceeds for the assessment of the level of randomness in a digital image. In the case of an ideal encrypted image, the entropy value should be close to

8, which is indicative of perfect randomness [9]. This has been conceived from the fact that many digital images have 8-bit intensity levels and contain (2^8 = 256) possible gray levels per pixel. Thus, an entropy value close to 8 signals that the encrypted image presents a maximum level of uncertainty and is unpredictable. In other words, it is an excellent signature indicating a good effective image encryption method.

$$H(M)= \sum_{i=0}^{N-1} p(M_x) \log_2 \frac{1}{M_x}$$

In this scenario, M_x stands for the pixel values, which for an 8-bit grey scale image range from 0 to 255; P(M_x) indicates the likelihood that the pixel value $M_x$will occur; and N indicates the total number of potential pixel values, which in the case of a greyscale image is 256.

IMAGE	Entropy (Original)	Entropy (Encrypted)
Peppers64	7.4935	7.9469
Peppers128	7.5491	7.9873
Peppers256	7.5689	7.9948
Peppers512	7.5945	7.9970
Barbara64	7.7524	7.9454
Barbara128	7.7583	7.9882
Barbara256	7.7558	7.9943
Barbara512	7.3438	7.9923
Lena64	7.2670	7.9534
Lena128	7.3915	7.9875
Lena256	7.4802	7.9962
Lena512	7.3479	7.9965

Table:3: Entropy Calculation of Gray Images Original Vs Encrypted

4.3 Corelation Coefficient:

Encrypting the original image and then utilising the correlation coefficient method to assess the encrypted version is a popular method for encrypting digital photographs. By examining the relationship between two variables—in this case, the pixel values of the original and encrypted images—the correlation coefficient is a statistical metric used to evaluate the efficacy of an encryption scheme. Complete decorrelation (perfect for encryption) is represented by a correlation coefficient of 0; perfect negative correlation is represented by a correlation coefficient of -1; and no encryption impact is implied by a correlation coefficient of 1.

$$r_{pq} = \frac{cov(p,q)}{\sigma_p \sigma_q} = \frac{\frac{1}{N_s}\sum_{i=1}^{N_s}(p_i - E(p))(q_i - E(q))}{\sqrt{\frac{1}{N_s}(p_i - E(p))^2}\sqrt{\frac{1}{N_s}(q_i - E(q))^2}}$$

IMAGE	Correlation-Coefficient Values

Peppers64	-0.0077
Peppers128	-0.0051
Peppers256	0.0001
Peppers512	0.0030
Barbara64	0.0022
Barbara128	0.0079
Barbara256	0.0008
Barbara512	0.0023
Lena64	0.0022
Lena128	0.0063
Lena256	-0.0033
Lena512	0.0004

Table: 4 Correlation Coefficient Values of Gray Images

Conclusion:

This study examined the application of various 2D chaotic maps for image encryption, demonstrating their effectiveness in securing digital images. By leveraging the higher number of control parameters available in 2D chaotic maps compared to their 1D counterparts, the encryption methods achieved enhanced complexity and robustness. Security evaluations, which included parameters like NPCR and UACI, showed that these encryption techniques are very robust and highly resistant to differential attacks and provide much randomness with encrypted images. More analyses about entropy, correlation coefficients have validated the resistivity of encryption techniques in statistical and visual attacks as well. The results clearly underpin the potential of such 2D chaotic maps not only for image encryption but also for more extensive digital watermarking applications, where secure data embedding is of utmost importance. Future development could be in the direction of how these methods can be extended up to higher-dimensional chaotic maps for efficiency and security enhancement over the increasing demands of present multimedia security challenges.

Reference:

1. Prathi Raghava Krishna, Ch.V.M. Surya Teja, Renuga Devi S, Thanikaiselvan V, “A chaos-based image encryption using Tinkerbell map functions”, IEEE Conference, 2018
2. Yeter ŞEKERTEKİN, Özkan ATAN, An Image Encryption Algorithm Using Ikeda and Henon Chaotic Maps, 2016
3. R. N. Ramakant Parida, Swapnil Singh, Chittaranjan Pradhan, Analysis of Color Image Encryption Using Multidimensional Bogdanov Map, 2021
4. Kunal Kumar Kabi, Chittaranjan Pradhan, Bidyut Jyoti Saha, Ajay Kumar Bisoi, Comparative study of Image Encryption using 2D Chaotic Map, 2014
5. Tejas Atul Dhopavkar, Sanjeet Kumar Nayak, Satyabrata Roy, IETD: a novel image encryption technique using Tinkerbell map and Duffingmap for IoT applications, 2022.
6. Swapnil Singh, Ramakant Parida and Chittaranjan Pradhan, Comparative Analysis of Image Encryption using 2D and 3D Variations of Duffing Map, International Conference on Communication and Signal Processing, 2018.

7. Ramakant Parida, Binod Kumar Singh, Chittaranjan Pradhan, Enhancing Image Security: A Hybrid Encryption Approach Incorporating Bogdanov and Duffing Maps with DWT, Vol. 45 No. 3 (2024).
8. Abbas, N.A.: Image encryption based on independent component analysis and Arnold's cat map. Egyptian informatics journal 17(1), 139–146 (2016)
9. Balaska, N., Ahmida, Z., Belmeguenai, A., Boumerdassi, S.: Image encryption using a combination of grain-128a algorithm and Zaslavsky chaotic map. IET Image Processing 14(6), 1120–1131 (2019)
10. Luo, Y., Yu, J., Lai, W., Liu, L.: A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications 78(15), 22023–22043 (2019)
11. Nayak, P., Nayak, S.K., Das, S.: A secure and efficient color image encryption scheme based on two chaotic systems and advanced encryption standard. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 412–418 (2018). IEEE
12. H. Xiang and L. Liu, "An improved digital logistic map and its application in image encryption," Multimed. Tools Appl., vol. 79, no. 41–42, pp. 30329–30355, Nov. 2020, doi: 10.1007/s11042-020-09595-x.
13. V. Kumar and A. Girdhar, "A 2D logistic map and Lorenz- Rossler chaotic system based RGB image encryption approach," Multimed. Tools Appl., vol. 80, no. 3, pp. 3749–3773, Jan. 2021, doi: 10.1007/s11042-020-09854-x.
14. Gururaj Hanchinamani and Linganagouda Kulakarni," Image Encryption Based on 2-D Zaslavskii chaotic Map and Pseudo Hadmard Transform", Vol.7, No.4 (2014), pp.185-200
15. N. K. Pareek, V. Patidar and K. K. Sud, "Image encryption using chaotic logistic map", Image Vision and computing, vol. 24, **(2006)**, pp. 926-934.
16. S. Sam, P. Devaraj and R. S. Bhuvaneswaran, "A novel image cipher based on a mixed transformed logistic map", Multimedia tools and applications, An international Journal, Springer, vol. 56, no. 2, **(2012)**, pp. 315-330.
17. Sudeshna Bora, Pritam Sen, Chittaranjan Pradhan, "Novel color image encryption technique using Blowfish and Cross Chaos map", ICCSP, DOI:10.1109/ICCSP.2015.7322621
18. Guan Zhi-Hong, Huang Fangjun, Guan Wenjie (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1- 3):153–157.
19. Chittaranjan Pradhan, Shibani Rath and Ajay Kumar Bisoi, "Non-Blind Digital Watermarking Technique Using DWT and Cross Chaos", 2nd International Conference on Communication, Computing & Security, Elsevier, vol. 6, 2012, pp. 897 – 904.
20. Alireza Jolfaei and Abdolrasoul Mirghadri," An Image Encryption Approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology", 2010, pp. 117-125.
21. Ramesh Kumar Yadava, Dr. B. K. Singh, S. K. Sinha and K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications, vol. 3, no. 6, 2013, pp. 14-20.

22. Musheer Ahmad and M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping",International Journal on Computer Science and Engineering, vol. 2(1),2009, pp. 46-50.
23. Jiri Fridrich," Symmetric Ciphers based on Two-Dimensional Chaotic Maps", International Journal of Bifurication and Chaos, vol. 8, no. 6,1998, pp. 1259-1284.
24. Jui Cheng and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption", International Symposium on Circuits and Systems, IEEE, 2000, vol.4, pp. 49–52.
25. Ye G, Wong KW (2012) An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn 69(4):2079–2087.
26. V. Patidar, N. K. Pareek and K. K. Sud, "A new substitution diffusion-based image cipher using chaotic standard and logistic maps", Communications in nonlinear science and numerical simulations, Elsevier, vol. 14, **(2009)**, pp. 3056-3075.
27. N. K. Pareek, V. Patidar and K. K. Sud, "Image encryption using chaotic logistic map", Image Vision and computing, vol. 24, **(2006)**, pp. 926-934.
28. Patro K, Banerjee A, Acharya B (2017) A simple, secure and time efficient multi-way rotational permutation and diffusion based image encryption by using multiple 1-D chaotic maps. In: International Conference on Next Generation Computing Technologies. Springer, Singapore, pp 396–418.
29. Wang, H., Xiao, D., Chen, X., Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map. Signal processing 144, 444–452 (2018).
30. Huang, C.-K., Liao, C.-W., Hsu, S., Jeng, Y.: Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommunication Systems 52(2), 563–571 (2013).
31. Subashini, V., Poornachandra, S.: Chaos based image encryption using bogdanov map. Journal of Computational and Theoretical Nanoscience 14(9), 4508–4514 (2017).
32. Mahdi, A., Jawad, A.K., Hreshee, S.S.: Digital chaotic scrambling of voice based on duffing map. International Journal of Information and Communication Sciences 1(2), 16–21 (2016).
33. Fu, C., Meng, W.-h., Zhan, Y.-f., Zhu, Z.-l., Lau, F.C., Chi, K.T., Ma, H.-f.: An efficient and secure medical image protection scheme based on chaotic maps. Computers in biology and medicine 43(8), 1000–1010 (2013).
34. Abbas, N.A.: Image encryption based on independent component analysis and Arnold's cat map. Egyptian informatics journal 17(1), 139–146 (2016).
35. Hassani, E., & Eshghi, M. (2013). Image encryption based on chaotic tent map in time and frequency domains. *The ISC International Journal of Information Security*,*5*(1), 97–110.
36. Wu, Y., Noonan, J. P. & Agaian, S. (2011). NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, 31-38.
37. Mahdi, A., Jawad, A. K., & Hreshree, S. S. (2016). Digital Chaotic Scrambling of Voice Based on Duffing Map. *Communications Engineering Journal*, *1*(2), 16–21.

38. Ahmad, M., & Alam, M. S. (2009). A New Algorithm of Encryption and Decryption of Images using Chaotic Mapping. *International Journal on Computer Science and Engineering*, *02*(01), 46–50.
39. Jain, A., & Rajpal, N. (2012). A two layer chaotic network based image encryption technique. *National Conference on Computing and Communication Systems*, 1-5.10.1109/NCCCS.2012.6413005
40. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.