An Integrated Arnold and Bessel Function-based Image Encryption on Blockchain

Abhay Kumar Yadav, Virendra P. Vishwakarma
University School of Information & Communication Technology,
Gobind Singh Indraprastha University, New Delhi 110078, India

***Abstract*—Images store large amount of information that are used in visual representation, analysis, and expression of data. Storage and retrieval of images possess a greater challenge to researchers globally. This research paper presents an integrated approach for image encryption and decryption using an Arnold map and first-order Bessel function-based chaos. Traditional methods of image encryption are generally based on single algorithms or techniques, making them vulnerable to various security threats. To address these challenges, our novel method combines the robustness of Arnold transformation with the unique properties of Bessel functions-based chaos. Furthermore, we implemented the decentralized nature of blockchain technology for storing and managing encryption keys securely. By utilizing blockchain's tamper-resistant and transparent ledger, we enhance the integrity and traceability of the encryption process, mitigating the risk of unauthorized access or tampering. The proposed method leverages the chaotic behavior of Bessel function for enhancing security of encryption process. A chaos obtained from first order Bessel function has been utilized for encryption key for encryption after Arnold transformation. The obtained cypher text is stored in blockchain in form of encrypted blocks for secured storage and added security. Experimental evaluations demonstrate the efficiency, effectiveness and robustness of our proposed encryption method when compared with performance of previously developed techniques highlighting the superiority of the proposed method in protecting image data against unauthorized access.**

Keywords*—Arnold transformation; block encryption; Bessel functions; blockchain

I. INTRODUCTION

Since digital image consists of large amount of distributed information, securing them is a major task for researchers. Also, digital images are less sensitive when compared with text data creating a minor change in image will create a drastic change in image pixels attribute. Digitized medical images provide an important aspect in storing patient's data as well as in diagnosing, treating and monitoring diseases [1].

The increasing amount of medical data generated by hospitals and clinics has led to the need for efficient storage and retrieval of these images [2]. Cloud storage services provide a reliable and cost-effective solution for storing large volumes of medical images. However, managing the security aspect of medical images stored in cloud is a major concern due to the personal and sensitive information of medical data [3]. Combining blockchain application with areas of medical research may provide newer potential in the biomedical field research. Sectors such as hospital and supply chain management of medicines and drugs may be benefitted from blockchain as it will impart a safer, secure, and reliable supply chain.

Blockchain technology can be used as a distributed electronic database encrypted by different cryptography functions thus eliminating existing limitations. Traditional systems use centralized authentication system making it difficult for various users to access database due to limited correct credential access and server capacity. Blockchain is similar to a distributed ledger, with different transactions encrypted together and, in the chain, and are permanent. Different features provided by blockchain have created newer use case application for cross integration with existing technologies for deployment across different domain. Researchers are working on enhancing these attributes for implementing them in image security [4]. Blockchain can work as a potential solution to the existing security issues in medical images.

The Arnold transformation represents a permutation-oriented cryptographic method designed to rearrange the pixel values within an image in a predictable yet intricate manner. This rearrangement instigates both confusion and dispersion, thereby fortifying the encrypted image against a spectrum of cryptographic assaults whereas, Bessel functions, a subset of mathematical special functions, are employed to add an additional layer of complexity to the transformed image. Through the application of Bessel functions, encryption is realized for each image by adapting the function's parameters dynamically in accordance with cryptographic keys. This combination approach enhances the overall security of the encryption scheme by customizing the encryption process for individual images

This paper aims to bridge the gap between the theoretical advancements in chaos theory, neural networks, and biological concepts, and their practical application in image security. By fusing these diverse elements into a unified framework, we strive to offer an innovative solution that addresses the challenges of image encryption in a rapidly evolving digital landscape. Through rigorous analysis and experimentation, we demonstrate the efficacy and robustness of the proposed Arnold Bessel-based framework for securing images.

The structure of this paper is arranged in following section: Section II highlights basic overview of the foundational concepts and related works. In Section III, the proposed methodology detailing the integration of Arnold maps and Bessel functions, Section IV delves into experimentation and

evaluation metrics. The results and discussions with previously developed techniques are also presented in this section. Section V discusses the storage on blockchain followed by conclusions and avenues for future research in Section VI.

II. BACKGROUND

A. Arnold Transformation

The Arnold Transform is a reversible image transformation used for image encryption. It is a simple and efficient algorithm that provides a level of security through its chaotic behavior. The Arnold Transform involves performing multiple iterations of a specific operation on image pixels to shuffle and disperse the pixel values, thus altering the image's appearance. This transformation can be used to encrypt an image, making it difficult for unauthorized users to understand the original content without the decryption process [5].

The Arnold transform is a chaotic transformation that can be used to scramble the pixels of an image, making it difficult to recognize. It is a simple transformation to implement, but it is very effective at disrupting the statistical properties of the image. Fig. 1 shows the distribution of image co-ordinates.

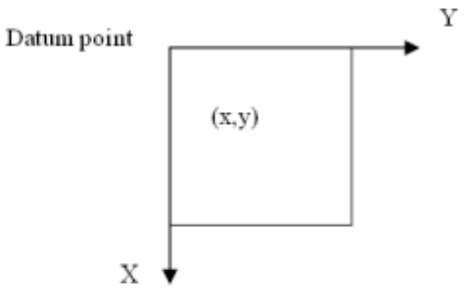

Fig. 1. Distribution of image coordinates.

The Arnold transform is area-preserving, meaning that it does not change the overall pixels in the image. However, it does scramble the pixels so that they are no longer correlated with their original positions [6]. Table I shows the scrambling cycle of Arnold transform based on size of image.

TABLE I. ARNOLD SCRAMBLING ALGORITHM CYCLE

Size of image (N)	Cycle of scramble (T)	Size of image (N)	Cycle of scrambling (T)
3	4	25	50
4	3	32	24
5	10	64	49
6	12	100	150
7	8	120	60

The Arnold transform works by taking the pixel coordinates (x, y) and transforming them to a new set of coordinates (x', y') using the following equations:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax & by \\ cx & dy \end{bmatrix} \text{mod M} \quad (1)$$

where a, b, c, and d are integer coefficients that satisfy the condition ad - bc = 1. M is the size of the image in pixels.

$$\begin{bmatrix} x_n + 1 \\ y_n + 1 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \begin{bmatrix} ab + 1 & -b \\ -a & 1 \end{bmatrix} \quad (2)$$

The Arnold Transform is a lightweight and fast encryption method, but it may not provide the same level of security as more complex encryption algorithms. Therefore, it is often used together with other encryption techniques for enhancing the security of image encryption applications [7].

B. Bessel's Function

The Bessel function is a mathematical function that plays a crucial role in various scientific and engineering applications, including the field of chaotic neural networks. The Bessel function can be used to create chaotic behavior within a neural network, which is desirable for certain applications that require randomness and unpredictability [8].

The Bessel function introduces non-linear dynamics into the neural network, resulting in complex patterns and behaviors. This chaotic behavior can enhance the network's capacity to process and analyze complex data, making it suitable for tasks such as image encryption and decryption [9].

In the process of creating a chaotic neural network using the Bessel function, the network's connections and weights are usually initialized randomly. As the network receives input data and performs computations, the Bessel function introduces non-linear transformations that lead to chaotic dynamics. This chaos can be harnessed to achieve desired behaviors, such as robust encryption and decryption of images. A generalized first order Bessel's Function is shown in Fig. 2.

The Bessel function can enhance the security and unpredictability of the encryption process. The complex and non-linear transformations introduced by the Bessel function make it challenging for unauthorized users to decipher the encrypted data without the proper decryption key [10].

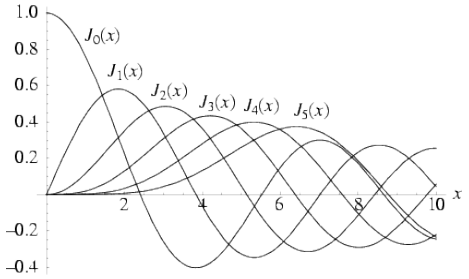

Fig. 2. Generalized representation of first order bessel's function.

III. METHODOLOGY

A. Previously Developed Techniques with Proposed Work

A detailed list of different encryption techniques presented by different researchers is listed in Table II.

B. Proposed Framework

Fig. 3 shows the methodology for the proposed framework followed by discussion on encryption and decryption techniques. The framework implements Arnold and Bessel's functions together for creating the chaotic encryption. The detailed algorithm for the encryption and decryption is mentioned in algorithm below.

Algorithm

Encryption

1. Arnold Map Transformation:

1.1 For each block of pixels in the image:
1.2 Apply the Arnold map transformation to the pixel coordinates.
1.3 Shuffle the pixels based on the transformed coordinates.

2. Bessel Function Key Generation:

2.1 Generate Bessel function coefficients using encryption parameters.

2.2. Create a set of Bessel functions based on the coefficients.

3. Pixel Transformation with Bessel Functions:

3.1 For each block of pixels in the image:

3.1.1. Apply a Bessel function transformation to the pixel values using the

generated Bessel functions.

3.1.2. Store the transformed pixel values in the encrypted image E.

Decryption

1. Pixel by pixel Bessel Decryption

The chaos generated after encryption are decoded back to obtain original image

2. Arnold Decoding

Images are descrambled for obtaining the original.

TABLE II. PREVIOUSLY DEVELOPED TECHNIQUES WITH PRESENTED TECHNIQUE

Techniques	Encryption Description	Technique
T1	1) Permutation by zig-zag pattern 2) Initial permutation from plain image Diffusion using XOR.	Zig-zag scan based chaotic feedback convolution model [11].
T2	1) DNA module based Intermediate Cypher image creation RNA module to produce final cypher image.	DNA rules, DNA-XOR operators and chaotic map [12].
T3.	1) Plain image hash value used for chaos generation Diffusion using DNA, XOR and RNA codons operations	Chaotic Evolutionary Biomolecules Model [13].
T4.	1) Plain image converted in DNA image by encoding rules 2) BST is created from DNA-BST is imposed on DNA image using XOR	BST, DNA coding, Logistic map [14].
T5.	1) Polynomial is selected by interval bisection at regular interval method creating sequence useful in encryption 2) Circular shift in confusion matrix Substitution matrix and masked image	bisection at interval method, Circular Shift, Substitution and XOR method [15].
T6.	1) Permutation by points obtained from Regula Falsi method 2) Encryption by image pixel substitution and iterative and cyclic shift.	Regula Falsi method, Substitution, Iterative addition, Circular Shift [16].
T7.	1) A unified key for selecting key pixels. 2) DNA encryption by pixel value substitution on key pixels Other pixels are encrypted by key stream of hyperchaotic Lorenz system	Key pixels, hyperchaotic Lorenz system scrambling, DNA encoding, Cyclic shift [17]
T8.	1) Fibonacci based pixels transformation 2) Scrambled image XOR with key image 3) Pixel values changed using Tribonacci Transform	Fibonacci and Tribonacci transformation [18].
Proposed	1) Image encryption by Arnold Transform. 2) A chaos obtained from first order Bessel function for encryption key for encryption at mid-level. 3) Storing the encrypted Data on blockchain for enhanced security	Arnold Transformation, Bessel Function, Blockchain

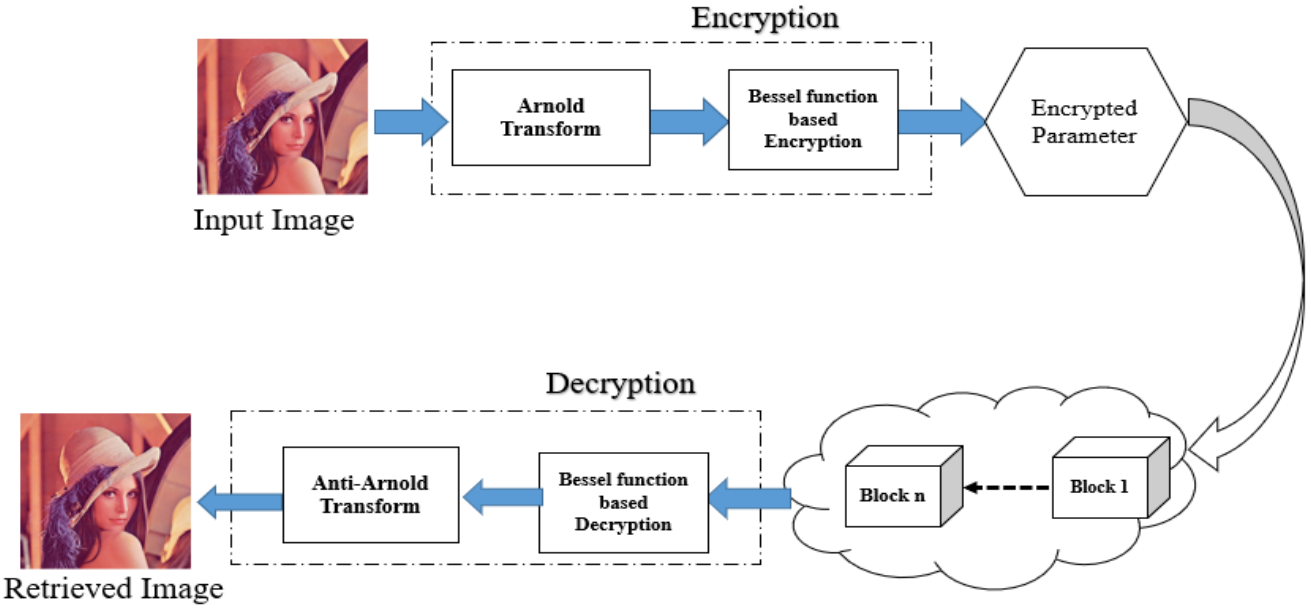

Fig. 3. Proposed Encryption and Decryption Framework

IV. Experimental Results and Performance Evaluation

The framework is executed using MATLAB R2023a software working on 64-bit machine with CPU Intel i9-4500U with 1.90 GHz processor and 8 GB RAM on Windows 11 OS. In the following section, the Lena image [19] is taken as the test image for evaluating our framework. Fig. 4 shows the different operations that are being performed on the test image.

To comprehensively evaluate the proposed framework, different performance evaluation measures are implemented working on following aspects: Entropy, execution time, correlation analysis. A detailed measures calculation and proposed methods results along with comparison with previously developed bench-mark approaches are presented in the Tables III, IV and V.

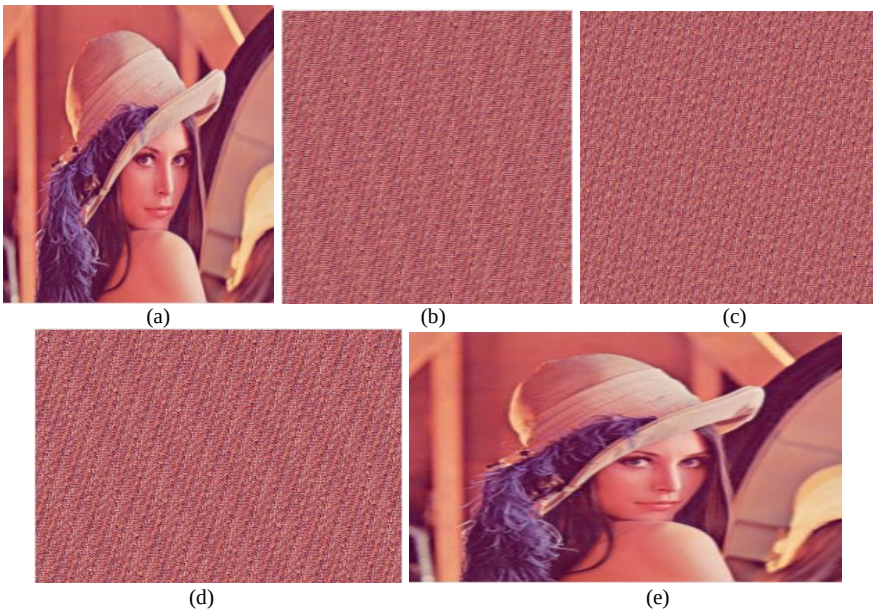

Fig. 4. Image storage and Retrieval a) Input Image b) Image after Arnold Transform c) Image after Arnold + Bessel d) Image Decryption after Bessel Arnold e) Retrieved Images.

TABLE III. PERFORMANCE COMPARISON IN TERMS OF CORRELATION COEFFICIENT

Method	Correlation Coefficient		
	Horizontal	Vertical	Diagonal
T1	-0.002062	0.003685	0.000249
T2	0.0054	0.0192	0.0055
T4	0.00007	0.0017	0.0008
T5	0.002097	0.002767	-0.0029
T6	0.001853	0.001984	0.000743
T7	-0.0026	-0.0033	0.0004
T8	-0.014825	-0.00066	0.007183
Proposed	0.00136	0.000217	0.00526

TABLE IV. PERFORMANCE COMPARISON IN TERMS OF EXECUTION TIME

Technique	Execution Time
T1	10. 440
T2	1.492
T3	3.009
T4	0.620
T5	0.798
T6	0.531
T7	0.288
T8	0.634
Proposed	3.687

TABLE V. PERFORMANCE COMPARISON IN TERMS OF ENTROPY

Technique	Entropy
T1	7.9994
T2	7.9994
T3	7.9995
T4	7.9992
T5	7.9993
T6	7.9994
T7	7.9993
T8	7.9994
Proposed	7.7634

The comparative analysis provides a holistic understanding of the strengths and limitations of the proposed integrated Arnold and Bessel function-based encryption scheme relative to existing methods. The comparisons highlight the superiority of the proposed framework in terms of entropy, execution time, and correlation analysis, reaffirming its efficacy in ensuring robust image encryption.

The results obtained from the comprehensive evaluation demonstrate that our proposed framework provide the expected encryption of images. On evaluation in terms of correlation coefficient, execution time and entropy showed the effectiveness and superiority of the proposed framework in achieving high levels of security and randomness in image encryption, thus validating its potential for practical deployment in real-world scenarios.

V. BLOCKCHAIN STORAGE

Ganache software [20] is capable of providing real-time simulation of smart contract executions based on Ethereum platform. Different use case and application can be simulated in Ganache based on its smart contract's features. Ganache provides 10 block free for mining and simulation, we have used only one block for storing the encrypted data obtained after the encryption process on Ganache software. Fig. 5 shows the working of Ganache software in storing encrypted parameters in detail with its implementation on front-end and back-end platform.

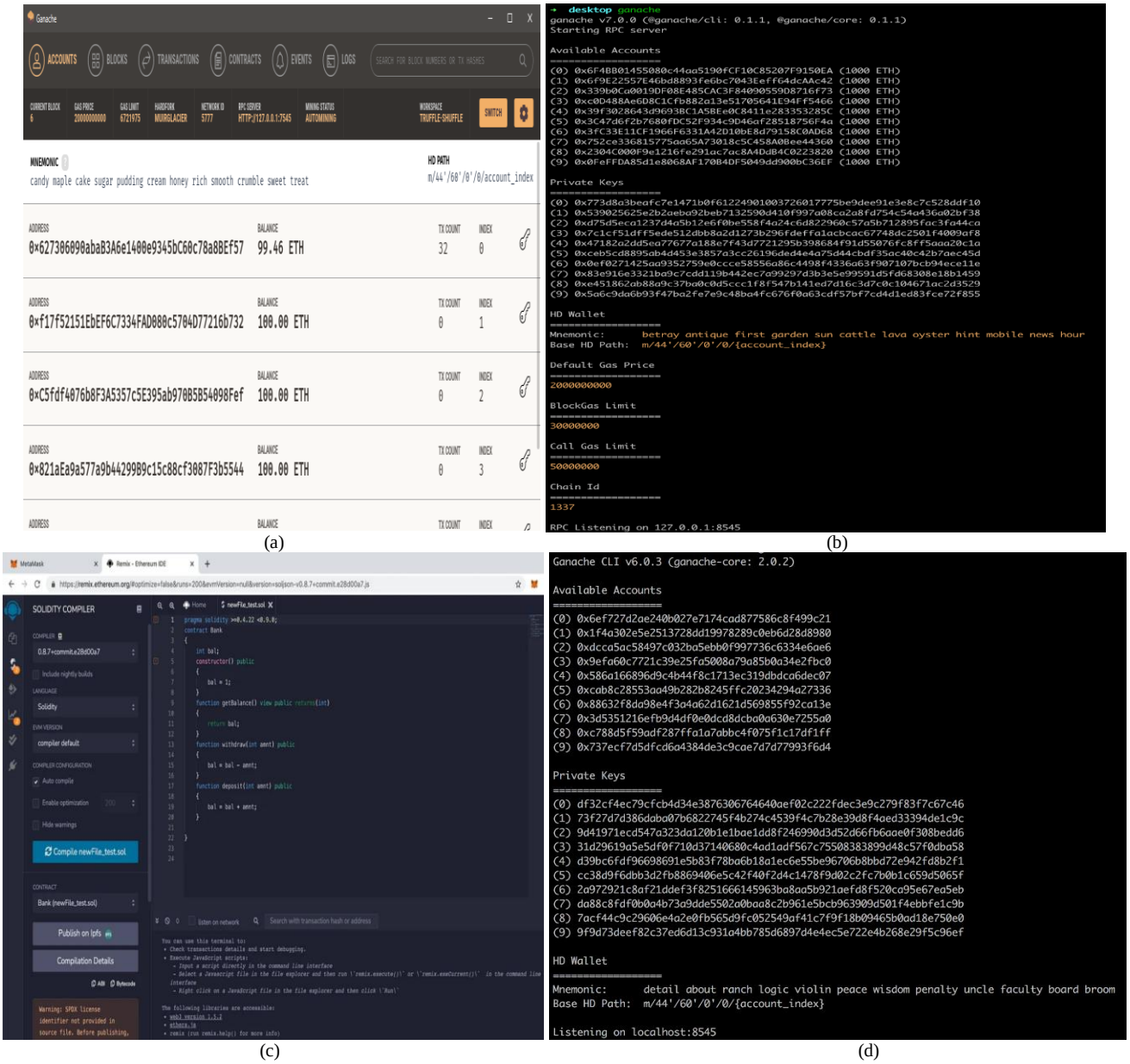

Fig. 5. Implementation on Ganache Framework a) Front End of Ganache Software b) Back-end on CLI interface c) Remix code for contracts d) Viewing all established contracts.

VI. Conclusion and Future Work

This paper proposes a new blockchain based image encryption framework with Arnold and Bessel's functions integration. This method obtains the encrypted data from the input image, store it on blockchain followed by decrypting it in reverse order to encryption to retrieve the original image. For performance evaluation, generic Lena image has been used for comparison with other encryption methods. The proposed work provides significant multi-level encryption and along with enhanced security. Its working has been validated with previously developed techniques.

In near future, more security techniques such as DNA barcoding can be further added for enhanced encryption. Moreover, chaos from neural networks can also be implemented for securing the images. The proposed framework can be implemented in medical images as they need proper encryption for securing patient's sensitive images.

Acknowledgment

Both authors acknowledge All India Council of Technical Education for the fellowship of first author under AICTE Doctoral Fellowship scheme.

References

[1] V. Narayan, M. Faiz, P.K. Mall, and S. Srivastava, "A Comprehensive Review of Various Approach for Medical Image Segmentation and Disease Prediction." *Wireless Personal Communications* 132, no. 3, pp. 1819-1848, 2023.

[2] V. Jeyakumar, K. Rama Abirami, S. Saraswathi, R. Senthil Kumaran, and G. Marthi, "Secure medical image storage and retrieval for Internet of Medical Imaging Things using blockchain-enabled edge computing." In *Intelligent Edge Computing for Cyber Physical Applications*, Academic Press, pp. 85-110, 2023.

[3] S. Kumar Jena, R. Chandra Barik, and R. Priyadarshini, "A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare." *Internet of Things*, 101111, 2024.

[4] ERD Villarreal, J García-Alonso, E Moguel, JAH Alegría, "Blockchain for healthcare management systems: A survey on interoperability and security." *IEEE Access* 11, pp. 5629-5652, 2023.

[5] R Yang, L Feng, J Li, "Image encryption based on 3D Arnold and elementary cellular automata method." *International Journal of Electronic Security and Digital Forensics* 16, no. 1, pp. 97-111, 2024.

[6] M Turan, E Gökçay, H Tora, "An unrestricted Arnold's cat map transformation, " *Multimedia Tools and Applications*, pp. 1-15, 2024.

[7] J Wu, Z Liu, J Wang, L Hu, S Liu, "A compact image encryption system based on Arnold transformation." *Multimedia Tools and Applications* 80, pp. 2647-2661, 2021.

[8] A Toktas, U Erkan, S Gao, C Pak", A robust bit-level image encryption based on Bessel map." *Applied Mathematics and Computation* 462, pp. 128340, 2024.

[9] SN Khonina, NL Kazanskiy, SV Karpeev, MA Butt, "Bessel beam: Significance and applications—A progressive review." *Micromachines* 11, no. 11, pp. 997, 2020.

[10] A Melman, O Evsutin "Methods for countering attacks on image watermarking schemes: Overview." *Journal of Visual Communication and Image Representation*, pp. 104073, 2024.

[11] R Vidhya, M Brindha, NA Gounden, "Analysis of zig-zag scan based modified feedback convolution algorithm against differential attacks and its application to image encryption." *Applied Intelligence* 50, pp. 3101-3124, 2020.

[12] M Yadollahi, R Enayatifar, H Nematzadeh, M Lee, JY Choi "A novel image security technique based on nucleic acid concepts." *Journal of Information Security and Applications* 53, p. 102505, 2020.

[13] A. Ali Abbasi, M Mazinani, R Hosseini, "Evolutionary-based image encryption using biomolecules and non-coupled map lattice." *Optics & Laser Technology* 140, p. 106974, 2021.

[14] H Nematzadeh, R Enayatifar, M Yadollahi, M Lee, G Jeong, "Binary search tree image encryption with DNA." *Optik* 202, p. 163505, 2020.

[15] P Biswas, S Kandar, BC Dhara, "An image encryption scheme using sequence generated by interval bisection of polynomial function." *Multimedia Tools and Applications* 79, pp. 31715-31738, 2020.

[16] A Paul, S Kandar, BC Dhara "Image encryption using permutation generated by modified Regula-Falsi method." *Applied Intelligence* 52, no. 10, pp. 10979-10998, 2022.

[17] M Li, M Wang, H Fan, K An, G Liu "A novel plaintext-related chaotic image encryption scheme with no additional plaintext information." *Chaos, Solitons & Fractals* 158, p. 111989, 2022.

[18] C Maiti, BC Dhara, S Umer, V Asari, "An Efficient and Secure Method of Plaintext-Based Image Encryption Using Fibonacci and Tribonacci Transformations." *IEEE Access*, 2023.

[19] W. K. Pratt, "Digital Image Processing: PIKS Inside, Third Edition," Wiley-Interscience, 2001.

[20] Mathur. G., GANACHE: A Robust Framework for Efficient and Secure Storage of Data on Private Ethereum Blockchains, (Version 1) available at Research Square https://doi.org/10.21203/rs.3.rs-3495549/v1, 2023.