International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

MEDICAL IMAGE ENCRYPTION THROUGH CHAOTIC ASYMMETRIC CRYPTOSYSTEM

E. MOUNIKA REDDY [1], PASUNUTI UDAYKIRAN [2], PULLURI VARSHINI [3], KOYYADA SAI VINEETH [4], PADAKANTI BHUVAN KUMAR [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In the era of digital advancements, safeguarding medical data holds significant importance. This article introduces a novel approach to encrypting images through public-key encryption, incorporating the properties of Elliptic Curve Cryptography (ECC) and the Blum-Goldwasser Cryptosystem (BGC). The proposed method capitalizes on the chaotic properties of a sequence generator to augment the randomness in the encrypted image. The encryption process initiates with a secure key exchange mechanism using elliptic curves and the Blum-Goldwasser Cryptosystem. Pixel randomization is achieved through a chaotic map, followed by encryption using ECC and BGC, which integrates the discrete logarithmic problem, probabilistic encryption, and the quadratic residuosity problem. Both ECC and BGC components contribute to unpredictability and complexity, fortifying the security measures. The amalgamation of these cryptographic techniques provides resilience against cyber threats such as brute-force attacks and differential cryptanalysis. Thorough simulations and performance assessments affirm the effectiveness and computational efficiency of this hybrid approach when compared to existing methods.

The experimental values of information entropy, average correlation, NPCR and UACI are 7.9998, 0.0010, 99.6901% and 33.5260% respectively. The total time taken

for the proposed methodology is 0.142 seconds. These values indicates that the proposed hybrid chaotic image encryption method displays promise for diverse applications.

Index Terms – Medical image encryption, public-key cryptography, Elliptic Curve Cryptography (ECC), Blum-Goldwasser Cryptosystem (BGC), differential cryptanalysis, brute-force attack resistance, information entropy, NPCR, UACI.

I. INTRODUCTION

In the landscape of contemporary medicine, medical imaging emerges as a cornerstone, empowering doctors to accurately pinpoint diseases, track the effectiveness of treatments, and strategize for medical procedures. These technological tools, which include a spectrum from X-rays to MRI scans, offer critical data about the internal workings and potential irregularities within the body that might remain undetected during a standard physical exam. Dental radiographs serve as essential tool in oral healthcare, providing insights into a patient's oral condition that go beyond what is observed in routine exams. These visual records are pivotal for precise assessments, formulating treatment strategies, and observing alterations in the oral cavity. Dentists depend on these radiographs to identify issues including decay, loss of bone density, the presence of cysts or tumors, and misalignment of teeth. In the realm of forensic science, the preservation and accessibility of dental X-ray archives are essential for the identification of individuals and aiding in criminal investigations. Upholding patient data protection and adherence to privacy laws is critical, necessitating secure data storage, transparent access procedures, and confidentiality measures, as unauthorized access to these images could have serious consequences. The healthcare sector confronts persistent cybersecurity threats, with medical images frequently targeted. This article introduces an encryption method to enhance the security of dental X-rays. This method combines elliptic curve cryptography and the Blum-Goldwasser cryptosystem to encrypt the images, augmented by a chaotic sequence generator to bolster randomness. Unlike recent encryption techniques relying solely on chaotic systems or enhancements to existing methods, our proposed approach not only enhances randomness but also ensures image security by introducing discrete logarithmic problem, probabilistic encryption, and the quadratic residuosity

problem into the encrypted image. Despite integrating ECC, BGC, and chaotic systems, our method demonstrates superior time performance compared to other encryption methods. Medical image encryption has gained paramount significance in the contemporary landscape. Over recent years, numerous image encryption methods have been introduced. Some researchers have prioritized optimizing the time required for the process, while others have directed their efforts toward expanding the storage capacities of established algorithms. Additionally, certain proposed approaches have centered on bolstering the overall security of these strategies. The research presents an encryption method for medical imagery using a fuzzy integer subset and Substitution-box (S-box) entries, followed by evaluations to assess their dependability and security effectiveness. This S-box is applied in a newly suggested encryption strategy for medical images. Reference introduced a hyperchaotic system, ImproBsys, and combines it with compressive sensing and public key elliptic curve encryption to enhance image security. The approach reduces data and transmission volumes in multi-image encryption while maintaining its benefits. However, encrypting more images may impact image restoration due to compression ratios. The presented pseudo-random-number generator by AbdElHaleem, Abd-El-Hafiz, and Radwan in offers a simple and efficient design. It consumes low computational resources, making it ideal for real-time applications. Elliptic curves prove suitable for Pseudorandom number generator (PRNG) design, inheriting security from the Discrete Logarithm Problem. The framework simplifies blocks for fast, secure bitstream output. This study introduces a novel image encryption approach combining elliptic curve ElGamal and chaotic theory. It uses a secure hashing algorithm (SHA-512 hash) for generating initial values, reducing pixel correlations, and resisting known plain-text and chosen plain- text attacks. The method involves scrambling, elliptic curve encryption, and chaos-based diffusion to enhance pixel distribution randomness in the final cipher. Ibrahim and Alharbi introduced an image encryption scheme using a dynamic S-box and a chaotic additive mask, demonstrating resilience against chosen plain-text and chosen cipher-text attacks. It employs secure techniques like random nonce and elliptic curve encryption for improved security.

II. RELATED WORK

A. *An integrated image encryption scheme based on elliptic curve*

Due to the extensive demand for digital images across all fields, the security of multimedia data over insecure networks is a challenging task. The majority of the existing modern encryption schemes are merely developed that ensure the confidentiality of the image data. This manuscript presents a new image encryption scheme that ensures confidentiality, user authentications, and secure key sharing among the communicating parties. Initially, the users share a secret parameter using Diffie-Hellman over the elliptic curve and pass it through SHA-256. Afterwards, the proposed scheme uses the first 128-bits for the confidentiality of the data, while the remaining 128-bits are for authentication. In the encryption algorithm, the confusion module is achieved by affine power affine transformation. At the same time, the diffusion module is attained through highly nonlinear sequences, which are generated through the elliptic curve. Experimental testing and the latest available security tools are used to verify the effectiveness of the proposed algorithm. The simulation findings and the comparison of the proposed scheme with the existing image encryption techniques reveal that the suggested scheme offers a sufficient degree of security.

Furthermore, the outcome of the simulation results divulges several advantages of the proposed scheme, including a large key space, resistance to differential attacks, high efficiency, and strong statistical performance.

B. *Improvement of image transmission using chaotic system and elliptic curve cryptography*

Recently, an encryption scheme based on chaotic and enhanced elliptic curve cryptography was proposed. The author uses a pixel grouping method as an essential stage for the entire encryption scheme. This Pixel grouping method is carried out so that the execution speed is enhanced. However, there exists a condition during the pixel grouping stage that makes the method futile while decrypting. Upon pixel grouping, if the large integer turns out to be equal or larger than the modulo prime parameter P of the elliptic curve, precise decrypted values cannot be obtained. In this paper, the flaw is avoided by using the inverse modulo operator if the large integer is greater than or equal to P. Experimental analysis to prove the conditions is shown in this paper. Moreover, a new method is added to circumvent such conditions.

C. *A novel image encryption scheme based on elliptic curves over finite rings*

Image encryption based on elliptic curves (ECs) is emerging as a new trend in cryptography because it provides high security with a relatively smaller key size when compared with well-known cryptosystems. Recently, it has been shown that the cryptosystems based on ECs over finite rings may provide better security because they require the computational cost for solving the factorization problem and the discrete logarithm problem. Motivated by this fact, we proposed a novel image encryption scheme based on ECs over finite rings. There are three main steps in our scheme, where, in the first step, we mask the plain image using points of an EC over a finite ring. In step two, we create diffusion in the masked image with a mapping from the EC over the finite ring to the EC over the finite field. To create high confusion in the plain text, we generated a substitution box (S-box) based on the ordered EC, which is then used to permute the pixels of the diffused image to obtain a cipher image. With computational experiments, we showed that the proposed cryptosystem has higher security against linear, differential, and statistical attacks than the existing cryptosystems.

D. *Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol*

For the asymmetric key, the Diffie Hellman Key (DHK) protocol is very efficient, but sometimes it is vulnerable against brute force attacks if the parameters are not chosen carefully. Our study aims to improve the asymmetric key scheme based on the elliptic curve cryptosystem (ECC). The sender and receiver agree on an elliptic curve based on the DHK sharing technique, but generator G is kept secret, and we generate its hash value, which is shared publicly. The authorized members can recover G using the hash value. By keeping G secret, the key protocol becomes much more robust than existing ones. Further, the proposed scheme will be applied to multiple RGB images. In this novel public key algorithm, 4D chaotic sequences are used for the diffusion of image pixels. The pixels' values are used for permutations of images rather than the chaotic sequences, strengthening the scheme against chosen/known plain text attacks. The simulation and the security analysis of the proposed algorithm show efficiency, potential to endure the varied attacks, and prospects for real-world application.

III. PROPOSED METHODOLOGY

This article introduces a novel approach to encrypting images through public-key encryption, incorporating the properties of Elliptic Curve Cryptography (ECC) and the Blum-Goldwasser Cryptosystem (BGC). The proposed method capitalizes on the chaotic properties of a sequence generator to augment the randomness in the encrypted image. The encryption process initiates with a secure key exchange mechanism using elliptic curves and the Blum-Goldwasser Cryptosystem. The healthcare sector confronts persistent cybersecurity threats, with medical images frequently targeted. This article introduces an encryption method to enhance the security of dental X-rays.

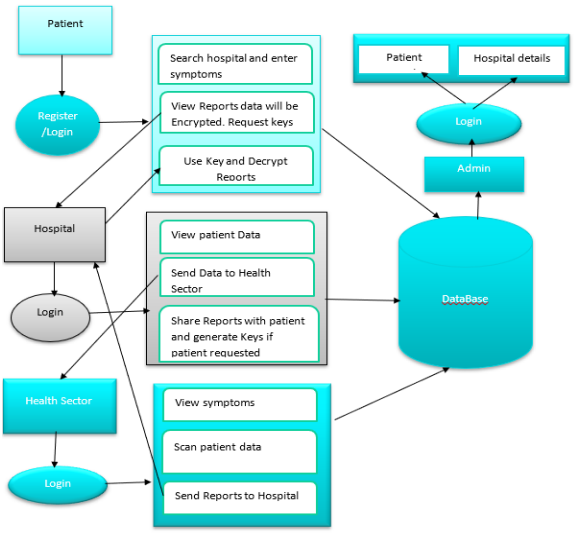
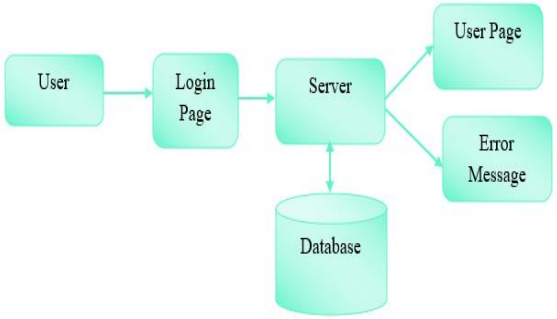


Fig. 1: System Overview

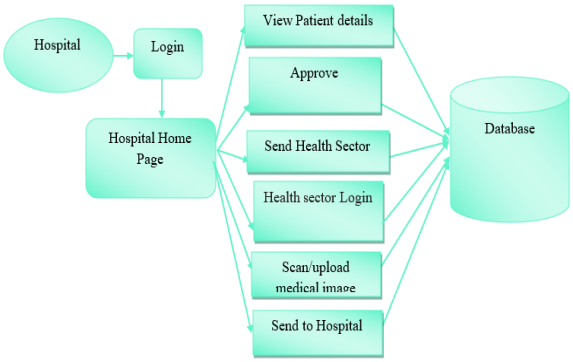
3.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



3.2 Hospital

Hospital is the second module in our project, Hospital first login with Username and password then view patient details and symptoms or request and approve the patient and join. After hospital management accepting the patient, he will view send the symptoms to health sector for scanning the patient and that data will be send to Hospital. Hospital management will send the reports to patient in encrypted format for security purpose. Patient have to request hos management and send keys to decrypt the reports.



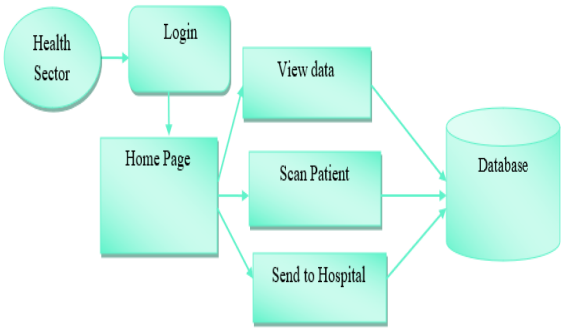
3.3 Admin

This is the third module in our project where Admin Controls all the of the project role. Administration managers ensure an organization's activities run smoothly and efficiently. The primary goals of an administration manager are to direct, control and supervise the support services of the organization to facilitate its success.



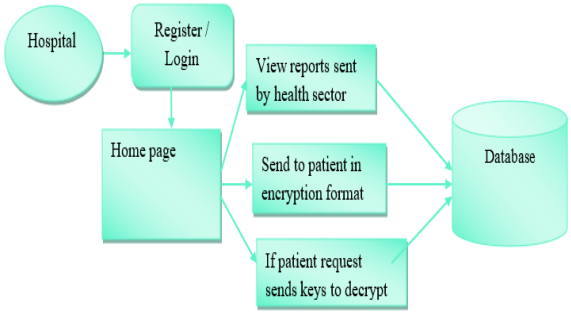
3.4 Health Sector

This is the fourth module in our project is Health Sector. Here Health Sector view patient symptoms where hospital management has sent. Based on patient data he will scan the patient and those reports as sent to Hospital Management.



3.5 Encryption

The encryption of medical images using Elliptic Curve Cryptography (ECC) and the Blum-Goldwasser cryptosystem provides a robust framework for ensuring the confidentiality and integrity of sensitive medical data. ECC offers a high level of security with smaller key sizes, making it ideal for resource-constrained environments typical in medical applications.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results demonstrate that the proposed medical image encryption method provides strong security and efficient performance. It achieved high entropy, very

low pixel correlation, and excellent NPCR and UACI values, showing strong resistance to statistical and differential attacks. The total encryption time of 0.142 seconds indicates that the method is fast and practical for real-time medical image protection.

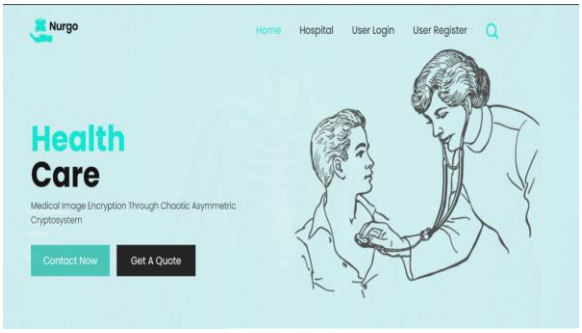


Fig. 2: Home Page

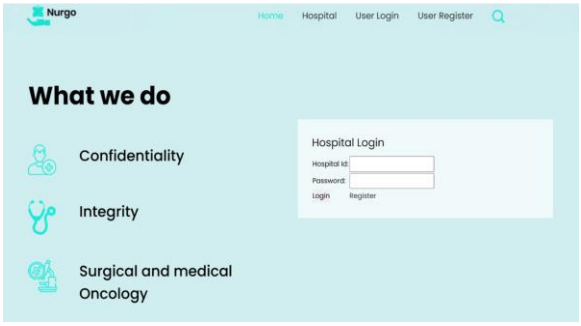


Fig. 3: Login

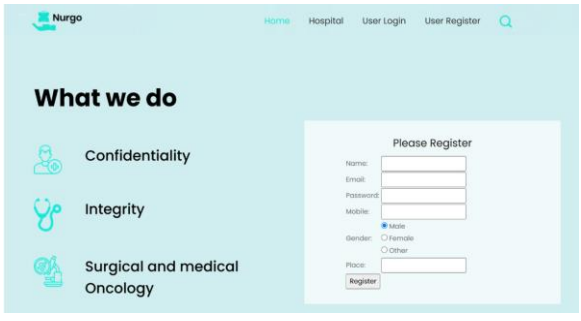


Fig. 4: User Registration

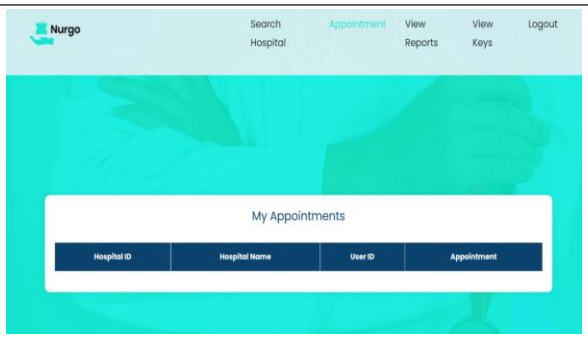


Fig. 5: Appoinments

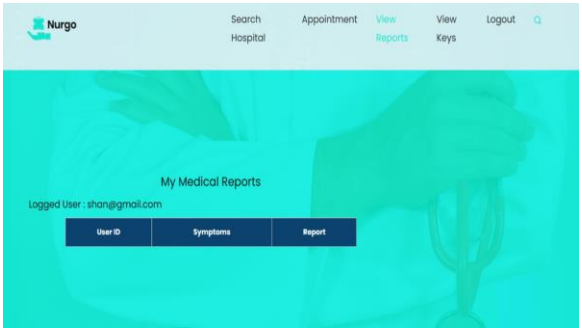


Fig. 6: Medical Reports

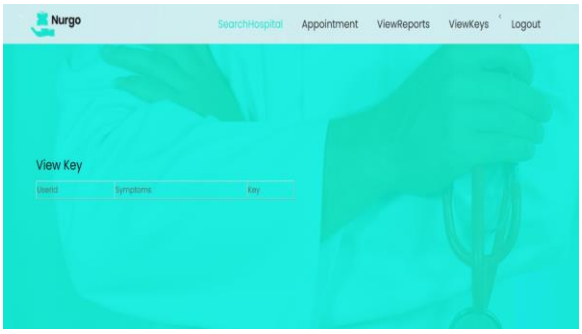


Fig. 6: Search Hospital

V. CONCLUSION

The proposed medical image encryption method, which integrates Elliptic Curve Cryptography (ECC) with the Blum-Goldwasser Cryptosystem, excels in both security and computational efficiency. Through meticulous comparison with

existing encryption techniques, our innovative approach proves to be notably more effective, particularly in terms of execution speed, with a total execution time of 0.142 seconds. The seamless integration of ECC's mathematical robustness and the stochastic properties of Blum-Goldwasser ensures a robust defence for digital images, meeting the contemporary need for swift and reliable data transmission. Its sensitivity to encryption keys, resilience against attacks, and comprehensive security measures either match or exceed those of current systems.

REFERENCES

[1] A. Razaq, L. A. Maghrabi, M. Ahmad, F. Aslam, and W. Feng, ''Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine,'' IEEE Access, vol. 12, pp. 7584–7608, 2024, doi: 10.1109/ACCESS.2024.3351794.

[2] G. Ye, M. Liu, and M. Wu, ''Double image encryption algorithm based on compressive sensing and elliptic curve,'' Alexandria Eng. J., vol. 61, no. 9, pp. 6785–6795, Sep. 2022.

[3] S. H. AbdElHaleem, S. K. Abd-El-Hafiz, and A. G. Radwan, ''A generalized framework for elliptic curves based PRNG and its utilization in image encryption,'' Sci. Rep., vol. 12, no. 1, p. 13278, Aug. 2022.

[4] Y. Luo, X. Ouyang, J. Liu, and L. Cao, ''An image encryption method based on elliptic curve ElGamal encryption and chaotic systems,'' IEEE Access, vol. 7, pp. 38507–38522, 2019.

[5] S. Ibrahim and A. Alharbi, ''Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography,'' IEEE Access, vol. 8, pp. 194289–194302, 2020.

[6] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, ''Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps,'' IEEE Access, vol. 9, pp. 76191–76204, 2021.

[7] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif, and I. Saddique, ''An integrated image encryption scheme based on elliptic curve,'' IEEE Access, vol. 11, pp. 5483–5501, 2023.

[8] M. Benssalah, Y. Rhaskali, and K. Drouiche, ''An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography,'' Multimedia Tools

Appl., vol. 80, no. 2, pp. 2081–2107, Jan. 2021.

[9] N. A. Azam, I. Ullah, and U. Hayat, ‘‘A fast and secure public-key image encryption scheme based on mordell elliptic curves,’’ Opt. Lasers Eng., vol. 137, Feb. 2021, Art. no. 106371.

[10] I. Khalid, S. S. Jamal, T. Shah, D. Shah, and M. M. Hazzazi, ‘‘A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes,’’ IEEE Access, vol. 9, pp. 77798–77810, 2021.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. PASUNUTI UDAYKIRAN pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. PULLURI VARSHINI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. KOYYADA SAI VINEETH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. PADAKANTI BHUVAN KUMAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Instit-

utions Technical Campus affiliated to JNTUH in 2022-2026.