IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 April 2024, accepted 18 May 2024, date of publication 22 May 2024, date of current version 3 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3404088

RESEARCH ARTICLE

Medical Image Encryption Through Chaotic Asymmetric Cryptosystem

TUTU RAJA NINGTHOUKHONGJAM, SURSITA DEVI HEISNAM, AND MANGLEM SINGH KHUMANTHEM
National Institute of Technology Manipur, Imphal, Manipur 795004, India
Corresponding author: Tutu Raja Ningthoukhongjam (ntsquare95@gmail.com)

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 Blum-Goldwasser cryptosystem, chaotic encryption, cryptanalysis, elliptic curve cryptography, image encryption, public key encryption.

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

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

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 [1] 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 [2] 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 [3] 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 [4] 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 [5] 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. The algorithm achieves high computational efficiency, with encryption speeds of approximately 60 MB/s, and can be extended to colour images. The image encryption and authentication model [6] employ chaotic 3D and 4D Arnold Cat maps to enhance encryption quality for grayscale and colour images. It results in higher entropy, lower correlation, improved security against chosen plain-text and known plain-text attacks, and overall stronger cipher images compared to existing methods. The research by Khalid et al. [7] introduces an image encryption scheme, ECIES (Elliptic Curve Integrated Encryption Scheme), combining symmetric encryption for diffusion and affine power transformation for confusion. The scheme utilizes a 128-bit symmetric key, with the first twelve bytes for diffusion and the remaining four bytes for confusion, enhancing image security. The study [8] presents an enhanced medical image encryption scheme for Telemedicine Information Systems (TMIS). Improvements include a more secure matrix key negotiation method via ECIES, an expanded self-invertible matrix for thwarting exhaustive search attacks, and the introduction of confusion and diffusion using Arnold's Cat map and hyperchaotic Lorenz generator, applicable to both grayscale and medical images. The paper [9] introduces a quick and reliable public-key encrypting strategy which is based on the principles of elliptic curves. It uses an efficient method to precompute a public elliptic curve, minimizing heavy computations. The scheme masks plain text pixels with random numbers and scrambles them with a dynamic S-box generated over two isomorphic elliptic curves. Advantages include efficient point generation, encryption, and high sensitivity to plain text for enhanced security. Complexity remains low and scales well with pixel count and symbol set size. This article [10] presents an asymmetric key cryptosystem using elliptic curves for digital image protection. The scheme employs substitution permutation networks with permutation achieved via elliptic curve mapping and S-boxes for confusion generation. Security analysis demonstrates resilience against entropy, brute force, and differential attacks, with efficient time complexity compared to existing encryption schemes. This work [11] introduces an asymmetric key cryptosystem based on elliptic curves for digital image layout security. The scheme uses newly constructed S-boxes derived from elliptic curves, which offer improved statistical and algebraic properties. The plain grayscale image is divided into blocks, and S-boxes enhance randomness and immunity against various attacks, ensuring security against entropy, brute force, and differential attacks. The paper by Kaur and Kumar [12] conducts an in-depth review of current image encryption techniques, categorizing them effectively. It highlights ongoing challenges like security vulnerabilities, parameter optimization, and computational speed. Researchers have introduced metaheuristic approaches, but they often face issues like slow convergence, premature convergence, and getting stuck in local optima. The study [13] presents an efficient and secure asymmetric image cipher for multiple colour images using elliptic curve cryptography and a 4D chaotic system. It combines input plain images, uses SHA-256 hashes to temper the chaotic system, performs XOR operations, and applies sensitive permutations. Elliptic curve encryption with an improved Diffie-Hellman key protocol enhances security, followed by a diffusion process. This paper [14] introduces a novel S-box generator and image encryption algorithm

using an elliptic curve over a ring of integers. The resulting S-box exhibits strong resistance to linear attacks. The scheme efficiently encrypts colour images with low run-time and high security, even for large images, where it demonstrates remarkable speed. The research [15] introduces an intensely concurrent mechanism for image encryption that utilizes parallel computational resources to diminish the timelines associated with encryption and decryption processes. It utilizes an elliptic curve-based chaotic system to eliminate sequential dependencies, achieving a speedup of 3.93 on a quadcore processor with a 98.3% parallelism efficiency. The scheme also enables partial image decryption, optimizing resource utilization. The paper [16] introduces an improved medical image encryption algorithm that combines elliptic curve cryptography with homomorphic encryption. It modifies traditional ECC to enhance key space and sensitivity. Experimental results demonstrate improved encryption and robustness against statistical and exhaustive attacks, making it a promising algorithm for medical image security.

The organization of this article is outlined as follows. A discussion on some fundamental preliminaries is given in Section II. The method proposed is detailed in Section III. The simulation is outlined in Section IV, along with an analysis of the results and a comparative study. Finally, Section V brings the paper to a close with the conclusion.

II. BASIC PRELIMINARIES

A. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a powerful and modern cryptographic technique that has gained significant attention in recent years due to its efficiency and security properties. Standing in contrast to the conventional cryptosystems, which are grounded on the principles of integer factorization, ECC depends on the mathematics of elliptic curves. This enables it to offer extensive security pivoting on small key sizes and efficient computational transactions. The essence of ECC is the mathematical characteristics of elliptic curves, regarded as algebraic frameworks delineated by equations comprising two variables. These curves showcase unique mathematical characteristics, marking them as appropriate for cryptographic purposes. ECC involves operations like point addition and scalar multiplication, executed on the points on these curves. These form the pillars of its encryption and decryption mechanisms. ECC features are extensively integrated into myriad security applications like secure communications, creation of digital signatures, and secure key exchange protocols.

An elliptic curve over a prime field is defined by the equation:

$$E\,(n, \alpha, \beta) = (x, y)\,|x, y \in Z \tag{1}$$

$$y^2 = x^3 + \alpha x + \beta \; mod\; n \cup O \tag{2}$$

where n is a prime number, $Z_{pn} = \{0,1,\ldots,n\text{-}1\}$ and α, $\beta \in Z_p$, with the condition,

$$4\alpha^3 + 27\beta^2 \neq mod\; n \tag{3}$$

'O' is the additive element, and called the "point at infinity." The inverse of a point P = (x, y) $\in E\,(n, \alpha, \beta)$ is:

$$-P = \begin{cases} 0, & if\ P = 0 \\ (x, n - y), & otherwise \end{cases} \tag{4}$$

For each pair of points, $P_1, P_2 \in E\,(n, \alpha, \beta)$, the sum of the points denoted by P_3=P_1+P_2, is defined as the inverse of the intersection of the line joining P_1 and P_2 with the curve.

$$P = \begin{cases} 0, & if\ P_1 = -P_2 \\ P_1, & if\ P_2 = 0 \\ P_2, & if\ P_1 = 0 \\ P_3\,(x_3\,, y_3), & otherwise \end{cases} \tag{5}$$

where,

$$x_3 = m_2 - x_1 - x_2 mod\; n \tag{6}$$

$$y_3 = m\,(x_1 - x_3) - y_1 mod\; n \tag{7}$$

$$m = \begin{cases} (y_2 - y_1)\,/\,(x_2 - x_1)\,, P_1 \neq P_2 \\ \left(3{x_1}^2 + \alpha\right)/2y_1, P_1 = P_2 \end{cases} \tag{8}$$

For a point $P_1 \in E(n, \alpha, \beta)$, and a multiplicand k $\in$Zp, kP_1 is defined as:

$$kP_1 = \begin{cases} 0, & if\ k = 0 \\ P_1 + P_1 + P_1 + \ldots\ldots k\ times, & if\ k \neq 0 \end{cases} \tag{9}$$

For two points P_1 and P_2 on the elliptic curve $E\,(n, \alpha, \beta)$, and $P_2 = kP_1$, one can calculate P_2 from k and P_1. However, it is very difficult to calculate k from P_1 and P_2. It is known as the elliptic curve discrete logarithm problem (ECDLP).

B. BLUM-GOLDWASSER CRYPTOSYATEM

Blum and Goldwasser [17] proposed an algorithm to encrypt data called the Blum-Goldwasser cryptosystem. It is a probabilistic, safe technique of encryption with a cipher text extension of fixed value. The encryption technique uses the Blum Blum Shub (BBS) pseudo-random number generator to create the key stream, which is an XOR-based stream cipher. Decryption is achieved by utilizing the secret key to manipulate the BBS generator's final state in order to spot the starting seed and reconstruct the plain-text. The cipher text of this method is just an additional amount longer than the message, the length k of n which is better compared to RSA algorithm. This is superior to bit-by-bit encryption's multiplicative expansion. For example, if we choose a 1024-bit modulus, the ciphertext will only be 128 bytes longer than the plain-text. A given plain-text may generate substantially different cipher-text each time it is encrypted since encryption is carried out using a probabilistic technique. The ability to prevent an adversary from deciphering intercepted messages by referring them to a dictionary of known cipher-text has many benefits.

C. JOANS-MURALIP'S MAP

JoanS-MuraliP's (JSMP) map by Muthu and Murali [18], is a one-dimensional chaotic map developed using the logistic map and a simple quadratic map. The novelty of the map lies in the exhibition of a large chaotic band of $0.502 \leq r \leq 2000$, which contributes to a large key space. The security analysis in reference [18] also reveals that the JSMP map demonstrates strong chaos and randomness. When compared to other existing one-dimensional maps, the JSMP map exhibits superior performance, making it well suited for implementing a robust encryption scheme. The Lyapunov exponent is a measure of the sensitivity to initial conditions in a dynamical system. Bifurcation is a phenomenon in dynamical systems theory where the behavior of a system undergoes a qualitative change as a parameter is varied. The Lyapunov Exponent comparison and the bifurcation plot of this map suggest the strong chaotic behavior of the JSMP map (FIGURE 1).
The map is denoted by the equation:

$$x_{n+1} = [r^2(x_n^2 - 5)(1 - r(x_n^2 - 5))] \, mod \, 1 \quad (10)$$

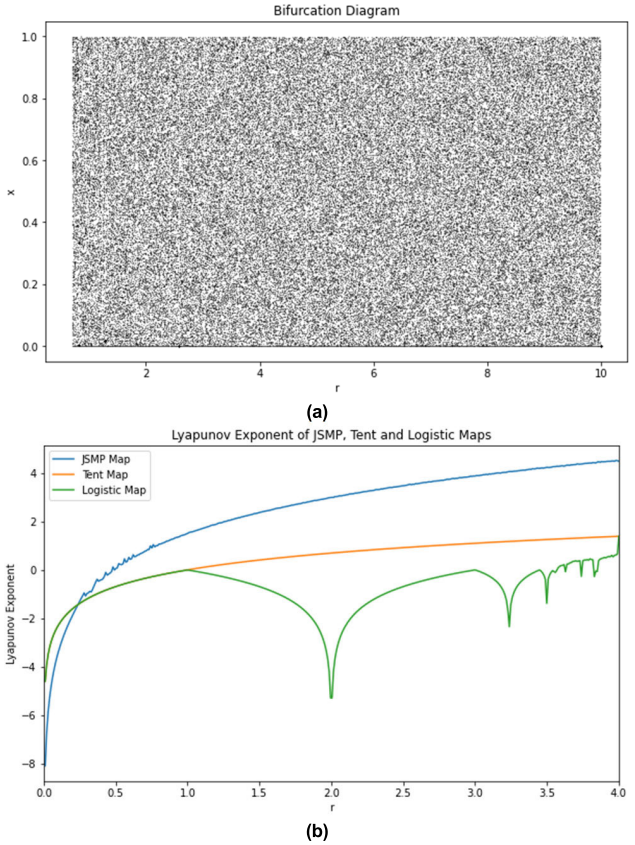


FIGURE 1. (a) Bifurcation diagram of JSMP map. (b) Comparison of Lyapunov exponents.

III. PROPOSED METHODOLOGY

The proposed approach encompasses three distinct algorithms (shown in FIGURE 2):

i. Key Generation, ii. Encryption, and iii. Decryption.

A. KEY GENERATION

Input: Prime numbers p, q, n.

Output: Public key and private key

1. First, choose two random and independent large prime numbers (256 bits) p and q, such that:

$$p, q \equiv 3 \, mod \, 4 \quad (11)$$

2. Value of m is calculated as:

$$m = p * q \quad (12)$$

3. Calculate the values of r and s using extended Euclidean algorithm, such that

$$r * p + s * q = 1 \quad (13)$$

4. Next, choose an Elliptic curve $E\ (\alpha, \beta, n)$,

$$y^2 = x^3 + \alpha x + \beta \, mod \, n \quad (14)$$

such that n>m. Here, n is the prime of the elliptic curve and point g is the base point of the curve.

5. Chooses a random number as the private key (pka) to generate a public key (pba) as:

$$pba = pka.g \quad (15)$$

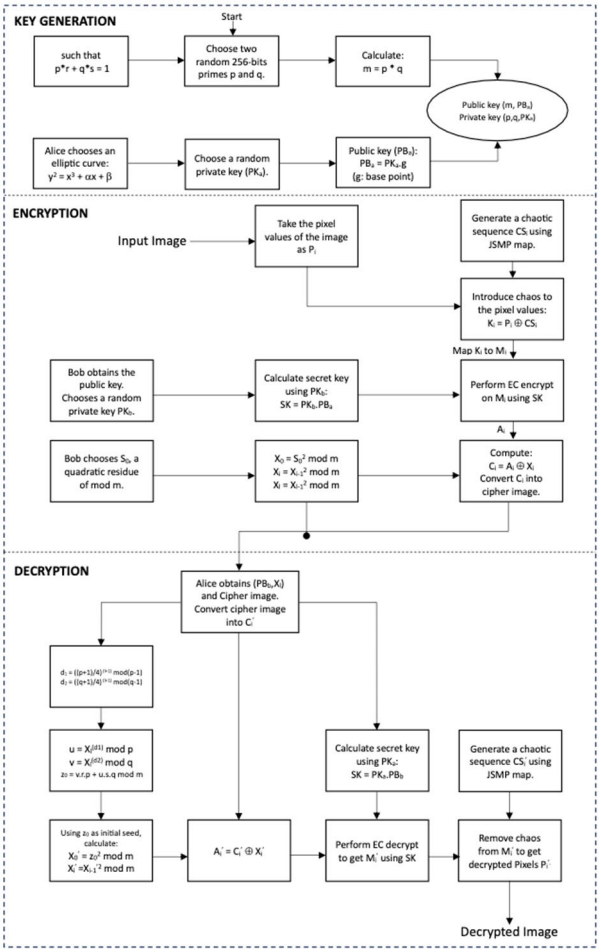


FIGURE 2. Proposed methodology.

6. Return the generated keys:
   Public key (m, pba).
   Private key (p, q, pka).

B. ENCRYPTION

Input: Public key and image.
Output: Cipher image.

1. Obtain the public key (m, pba).
2. Then choose a random number as private key (pkb).
3. Using pkb, calculate the shared secret key using the receiver's public key (pba) as:

$$Sk = pkb.\, pba \tag{16}$$

4. Use JSMP map to create a sequence of chaotic numbers J_i of length x (x= number of pixels).
5. Perform:

$$K_i = J_i \oplus P_i \tag{17}$$

   where P_i is the individual pixels of the image.
6. Make all the K_i values into strings of length 3 by adding '0' or '00' wherever necessary.
7. Using all these strings, make a string of length 156.
8. Convert the strings into its corresponding integer (M_i) of length l.
9. Bob then chooses a seed s_0, a random quadratic residue mod m to calculate x_0 as:

$$x_0 = s_0^2 \, mod \, m \tag{18}$$

10. Compute:

$$x_i = x_{(i-1)}^2 \, mod \, m \tag{19}$$

11. For the length of the mapped message (l), the following operations are performed:

$$\text{a. } A_i = M_i.Sk \, mod \, n \tag{20}$$

$$\text{b. } c_i = A_i \oplus x_i \, mod \, n \tag{21}$$

12. Compute:

$$x_l = x_{(l-1)}^2 \, mod \, m \tag{22}$$

13. Convert ci to cipher image and send to the receiver as:

$$(cipher\_image,\ x_l,\ pbb) \tag{23}$$

   where pbb is the public key of the sender.

C. DECRYPTION

Input: Cipher ($cipher\_image$, xl, pbb).
Output: Deciphered image.

1. First, the value of d_1 and d_2 are calculated by Alice using the private key (p, q):

$$d_1 = \left(\frac{p+1}{4}\right)^l mod(p-1) \tag{24}$$

$$d_2 = \left(\frac{q+1}{4}\right)^l mod(q-1) \tag{25}$$

2. Using the last value of the cipher text (x_l), Alice then calculates the value of u and v:

$$u = y\,(d_1)^l \, mod \, p \tag{26}$$

$$v = y\,(d_2)^l \, mod \, q \tag{27}$$

3. The initialization value of the sequence generator z0, is calculated as:

$$z_0 = vrp + usq \, mod \, m \tag{28}$$

4. Using z_0, an array of random number $x_i^{'}$ is generated as:

$$x_0^{'} = z_0^2 \, mod \, m \tag{29}$$

$$x_i^{'} = x_{(i-1)}^2 \, mod \, m \tag{30}$$

5. For the (l – 1), where l is the length of the cipher, Alice computes the following:
   (a)

$$A_i^{'} = c_i \oplus x_i^{'} \, mod \, n \tag{31}$$

   (b)

$$M_i^{'} = A_i^{'} S_k^{-1} \, mod \, n \tag{32}$$

6. Remove chaos from M_i' using JSMP map.
7. Map the result to decrypted image

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed method is executed on Dell Precision 7920 with 256 GB memory. The program was run on Spyder (with python 3.10.9). The dental x-ray (720x330) used to perform the encryption is obtained locally and the standard images, each of 512x512 size, were selected from the USC-SIPI image library for further testing.

In an elliptic curve E(a,b,p,g,n,h), where a and b are the constants (α and β) in equation 2, p is a prime which is the size of the field, g is a point on the curve known as the generator (also base point), n is the size of the subgroup and h is the cofactor. The parameters of the elliptic curve used are given below:

$a = -3$

b = 1 093 849 038 073 734 274 511 112 390 766 805 569 936 207 598 951 683 748 994 586 394 495 953 116 150 735 016 013 708 737 573 759 623 248 592 132 296 706 313 309 438 452 531 591 012 912 142 327 488 478 985 984

p = 864 797 660 130 609 714 981 900 799 081 393 217 269 435 300 143 305 409 394 463 459 185 543 183 397 656 052 122 559 640 661 454 554 977 296 311 391 480 858 037 121 987 999 716 643 812 574 028 291 115 057 151

g = (661 740 802 050 217 063 228 768 716 723 360 960 729 859 168 756 973 147 706 671 368 418 802 944 996 427 808 491 545 080 627 771 902 352 094 241 225 065 558 662 157 113 545 570 916 814 161 637 315 895 999 846, 3 757 180 025 770 020 463 545 507 224 491 183 603 594 455 134 769 762 486 694 567 779 615 544 477 440 556 316 691 234 405 012 945 539 562 144 444 537 289 428 522 585 666 729 196 580 810 124 344 277 578 376 784)

n = 6 864 797 660 130 609 714 981 900 799 081 393 217 269 435 300 143 305 409 394 463 459 185 543 183 397 655 394 245 057 746 333 217 197 532 963 996 371 363 321 113 864 768 612 440 380 340 372 808 892 707 005 449

h=1

In a series of tests, it was discovered that the optimal initial parameters to generate a chaotic sequence with a high level of chaos using the JSMP chaotic map (equation 10) are found at:

'r' in range (8.0 – 8.9). The initial parameter a_0 is calculated using the secret key Sk.

The performance analysis of the implemented method is given in TABLE 1.

TABLE 1. Performance analysis.

Metrics	Test values
Entropy	7.9998
Plain vs encrypted image:	
PSNR	8.6138 dB
SSIM	0.02
Plain vs decrypted image:	
PSNR	∞
SSIM	1
Correlation coefficients:	
Horizontal	-0.0009
Vertical	-0.0009
Diagonal	-0.0013
Key space	2^{1024}
NPCR %	99.6901
UACI %	33.5260

A. ENTROPY ANALYSIS

Entropy is used to quantify the level of unpredictability in data produced by a system. It plays a crucial role in gauging the effectiveness and safety of the information. A superior cipher text is typically associated with a higher entropy value. In the context of images, an encryption scheme shows exceptional performance when the raw image perfectly matches the decrypted version. The Peak Signal to Noise Ratio (PSNR) is an indicator that expresses the proportion amidst the mean squared deviation among pixel values present in two contrasting images, and the maximum possible mean squared discrepancy that can be observed between any two images. In the context of a cipher image, the PSNR value is typically anticipated to be on the lower end. On the other hand, the Structural Similarity Index (SSIM) is a metric that quantifies the degree of resemblance between two images. The SSIM value could vary from -1 to 1, with the value of 1 denoting that the two images under comparison are identical. Table 2 displays the comparison of PSNR, SSIM of encrypted image and decrypted image. The entropy value is compared with other similar methods in Table 4. The information entropy (E) is calculated using equation (33).

$$E = -\sum_{i=0}^{255} P(p_i)\log_2 P(p_i) \tag{33}$$

where, p_i, i are the pixel values of the image and $P(p_i)$ is the probability of the occurrence of the pixels.

The information entropy of any good encryption must be as close to 8. The entropy of the encrypted image produced by the proposed method is 7.9998.

TABLE 2. Comparison of PSNR and SSIM of encrypted images and decrypted images.

	Encrypted image PSNR (dB)	Encrypted image SSIM	Decrypted image PSNR (dB)	Decrypted image SSIM
Proposed (dental x-ray)	8.6138	0.002	∞	1
Proposed (mandrill)	8.7258	0.001	∞	1
Reference [19]	8.7733	0.006	31.06	0.58
Reference [20]	8.3431	0.008	∞	1
Reference [21]	8.8431	0.009	∞	1
Reference [22]	8.7854	0.009	∞	1
Reference [23]	8.6431	0.008	∞	1
Reference [24]	8.3451	0.008	∞	1
Reference [25]	8.7754	0.007	∞	1

B. HISTOGRAM ANALYSIS

A histogram represents pixel intensity distribution in an image. In a plain image, the histogram reflects content with peaks corresponding to colours. In encrypted images, histograms should appear more uniform, with fewer distinct peaks, as encryption aims to eliminate patterns and make it challenging to discern the original content. (FIGURE 3 shows the pixel distribution of the plain image and encrypted image).

C. KEY SPACE ANALYSIS

Elliptic Curve Cryptography provides better protection to the encrypted data than other techniques using the same key size. For standard ECC using a prime field F_p with a prime curve.p of 512 bits, the key space is approximately 2^{512}. This is derived from the number of possible private keys, which are integers in the range [1, p-1].

During the key generation process, two additional 256-bit primes, p and q, are used to generate m (a component of the public key).

Therefore, the resultant key space of the proposed method can be calculated as:

ECC key space = 2^{512}

Additional key space (p and q) = $2^{256} * 2^{256}$

Combined key space = $2^{512} * (2^{256} * 2^{256}) = \mathbf{2}^{1024}$

This key space is considered to be good enough to resist against any brute force attacks (comparison in TABLE 3).

TABLE 3. Comparison of key space.

Proposed Method	Ref [4]	Ref [5]	Ref [6]	Ref [7]	Ref [9]	Ref [15]	Ref [16]	Ref [25]
$\mathbf{2^{1024}}$	2^{564}	2^{208}	2^{512}	2^{128}	2^{512}	2^{507}	10^{128}	2^{772}

Ref = Reference

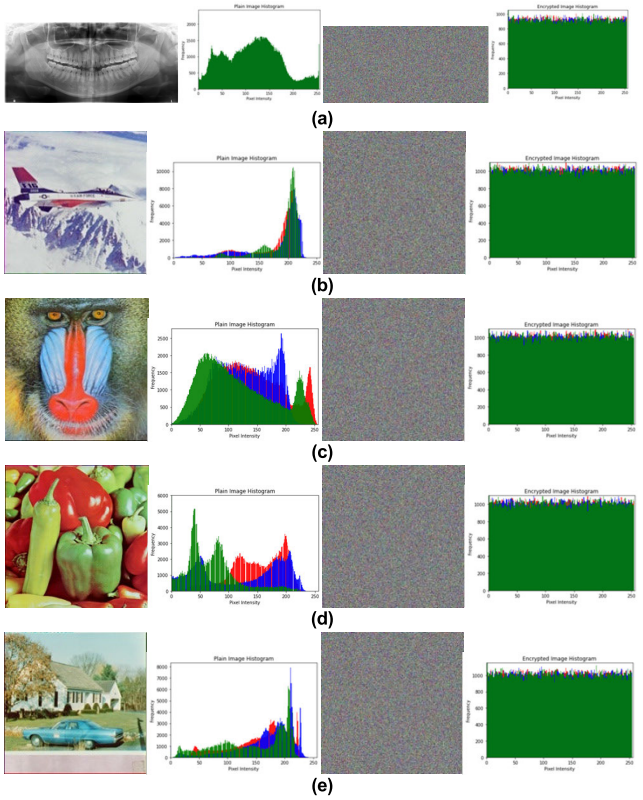


FIGURE 3. Plain image, corresponding histogram, encrypted image and corresponding histogram of (a) Dental x-ray, (b) Airplane, (c) Mandrill, (d) Peppers, (e) House.

D. CORRELATION ANALYSIS

Unencrypted images typically display uniformity with strong pixel correlations along the horizontal, vertical, and diagonal axes. In image encryption, high correlations between the original and encrypted images pose a security risk, potentially exposing patterns. A low correlation coefficient is vital in image encryption to enhance security by minimizing information retention from the original image (FIGURE 4). The correlation coefficient is calculated using the below equation (34):

$$Cc\,[v1,\ v2] = \frac{\text{Covariance}\,[\text{v1, v2}]}{SD\,[v1] \times SD\,[v2]} \tag{34}$$

where,

Cc: Correlation coefficient.

SD: Standard Deviation.

The correlational coefficients of the proposed method are compared with other existing similar methods in Table 4.

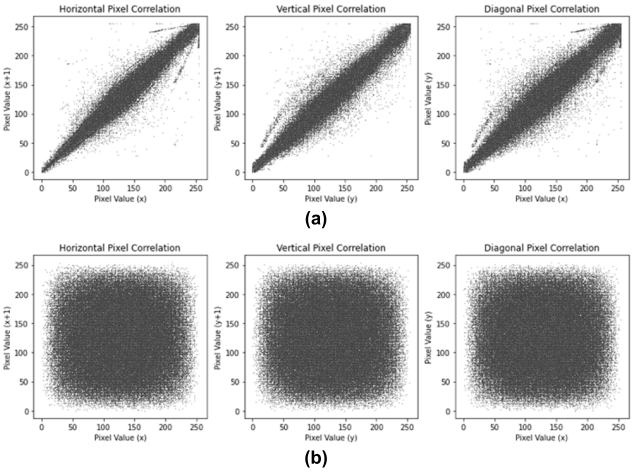


FIGURE 4. Horizontal, vertical and diagonal correlation plot for (a) plain dental x-ray. (b) encrypted dental x-ray.

E. KEY SENSITIVITY ANALYSIS

To test the key sensitivity of a method, we can alter the original key by a very small value and check whether the output is different from the output given by the original key. Difference between decrypted images using correct key and wrong key is shown in FIGURE 5. This shows that the proposed method is sensitive to even minute changes to the key.

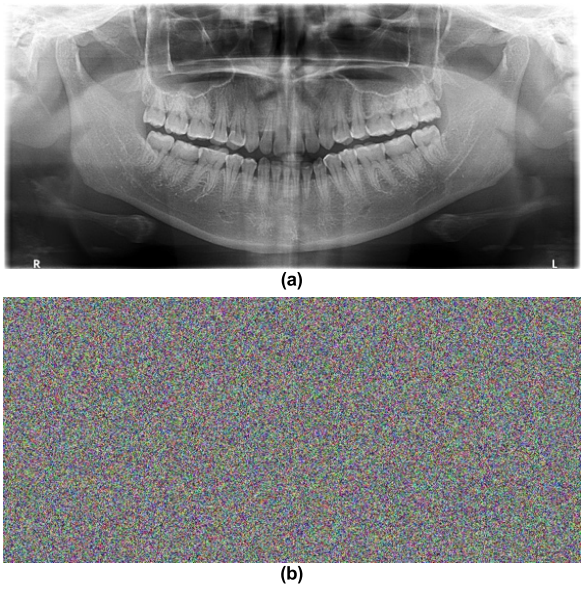


FIGURE 5. Decrypted images using: (a) correct key. (b) wrong key.

F. ECC ATTACKS ANALYSIS

1) KNOWN PLAIN-TEXT ATTACK

In a known plain-text attack, the attacker has the knowledge of a plain text and the cipher text. The values of the key may be extracted using this information. Each time a communication is encrypted, however, a new key is generated. As a result, known plain-text attack will fail.

TABLE 4. Comparison of entropy and correlation coefficients.

	Entropy	Horizontal correlation	Vertical correlation	Diagonal correlation
Proposed (dental x-ray)	7.9996	-0.0009	-0.0009	-0.0013
Proposed (mandrill)	**7.9998**	-0.0006	-0.0006	-0.0008
Reference [1]	7.9983	-0.0032	-0.0032	-0.0032
Reference [2]	7.9976	0.0043	-0.0118	-0.0116
Reference [3]	7.9970	0.0042	0.0009	0.0010
Reference [4]	7.9993	-0.0024	0.0031	-0.0013
Reference [5]	7.9973	0.0021	0.0117	0.0125
Reference [6]	7.9993	-0.0015	0.0047	0.0017
Reference [7]	7.9991	0.0044	0.0004	0.0091
Reference [8]	7.9970	0.0001	0.0005	0.0015
Reference [9]	7.9971	-0.0036	-0.0031	-0.0030
Reference [10]	7.9975	-0.0090	-0.0079	-0.0032
Reference [11]	7.9974	-0.0012	-0.0014	0.0016
Reference [13]	7.9992	0.0007	0.0049	0.0006
Reference [14]	7.9993	-0.0006	-0.0009	-0.0005
Reference [15]	7.9993	-0.0036	-0.0005	0.0003
Reference [16]	7.9700	0.0041	0.0022	0.0018
Reference [19]	7.9993	-0.0043	0.0014	0.0048
Reference [20]	7.9993	0.0124	-0.0118	-0.0215
Reference [21]	7.9993	0.0011	-0.0013	0.0022
Reference [22]	**7.9998**	-0.0040	-0.0040	-0.0040
Reference [23]	7.9990	-0.0013	0.0025	0.0014
Reference [24]	7.9970	-0.0021	-0.0061	-0.0068
Reference [25]	7.9991	-0.0015	-0.0005	-0.0034

2) KNOWN CIPHER-TEXT ATTACK

The attacker in a cipher text attack possesses both the encryption technique and the cipher text. The encrypted text cannot be translated to plaintext since the attacker does not know the receiver's private key. Furthermore, because to the massive size of the key, a brute force attack will take a long time.

3) POLLARD'S RHO ATTACK

Pollard's Rho method is one of the most well-known attacks on the elliptic curve cryptography. In this attack the private key can be found in at most square root of 'n' steps, where n is the cyclic order of the chosen curve. In this method, the generator of the curve is 'g'. The cyclic order n is calculated using g.

$$order = 6.8647976601 * 10^{156}$$

Therefore, the number of steps required to calculate private key is:

$$sqrt(order) = 2.620075888 * 10^{78}$$

TABLE 5. Comparison of NPCR and UACI values.

	NPCR (in %)	UACI (in %)
Proposed Method	99.6901	33.5260
Reference [1]	99.5911	33.5260
Reference [2]	99.5424	33.5112
Reference [3]	99.6063	33.4085
Reference [4]	99.5796	33.4296
Reference [5]	99.6086	33.4409
Reference [6]	99.6200	33.2830
Reference [7]	99.6402	33.3985
Reference [8]	99.6541	33.4615
Reference [9]	99.6200	33.3400
Reference [10]	99.6634	33.7112
Reference [11]	99.6100	33.6500
Reference [13]	99.6297	33.4083
Reference [14]	99.6100	33.4100
Reference [15]	99.6095	33.4621
Reference [16]	99.1800	38.5900
Reference [19]	99.7348	33.6878
Reference [20]	99.6100	33.5000
Reference [21]	99.6096	33.4599
Reference [22]	99.8324	33.3524
Reference [23]	99.6200	33.2800
Reference [25]	99.6100	33.4600

G. DIFFERENTIAL ATTACK ANALYSIS

Two important metrics used to assess the resistance of an encryption algorithm against differential attacks are the Normalized Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). NPCR and UACI are used to quantify the sensitivity of an encryption algorithm to changes in the plaintext. Lower UACI and higher NPCR values indicate a more secure algorithm against differential attacks, as they suggest that small changes in the plaintext result in more significant changes in the ciphertext (Table 5 shows the NPCR and UACI values). These values can be calculated using (equations 35-37):

$$D(i,j) = \begin{cases} 0, & I_1(i,j) = I_2(i,j) \\ 1, & I_1(i,j) \neq I_2(i,j) \end{cases} \quad (35)$$

$$NPCR = \frac{\sum_{i=1}^{l} \sum_{j=1}^{b} D(i,j)}{l \times b} \times 100\% \quad (36)$$

$$UACI = \frac{\sum_{i=1}^{l} \sum_{j=1}^{b} |I_1(i,j) - I_2(i,j)|}{l \times b \times 255} \times 100\% \quad (37)$$

where,

D(i,j) is a binary indicator function that determines whether the pixel values at (i,j) are different between two images.

I_1 and I_2 are the two ciphered images.

l and b are the dimensions of the images.

TABLE 6. Comparison of time performance.

	Encryption time (in seconds)	Decryption time (in seconds)	Total time (in seconds)
Proposed Method (dental x-ray)	**0.076**	**0.066**	**0.142**
Proposed Method (mandrill)	**0.078**	**0.072**	**0.150**
Reference [1]	-	-	0.4646
Reference [4]	1.812	-	-
Reference [5]	0.193	-	-
Reference [7]	0.213	-	-
Reference [8]	1.260	-	-
Reference [13]	0.704	-	-
Reference [15]	0.440	-	-
Reference [19]	0.380	0.280	0.660
Reference [20]	0.8175	1.3667	2.1842
Reference [21]	-	-	7.305
Reference [22]	0.350	0.280	0.630
Reference [23]	0.450	0.320	0.770
Reference [25]	0.680	0.710	1.390

H. TIME PERFORMANCE ANALYSIS

The proposed algorithm has undergone thorough comparison with existing similar techniques, demonstrating markedly better efficiency in terms of execution time. Through detailed benchmark tests, it has consistently surpassed the performance of other methods. This benefit is especially crucial in situations that demand quick processing, like those found in real-time applications. Table 6 shows the time taken for encryption and decryption of some methods.

V. CONCLUSION AND FUTURE SCOPE

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. However, a potential drawback of this method lies in its susceptibility to future quantum attacks. As digital technologies advance, our proposed solution presents an enticing alternative, striking an optimal balance between speed and security, thus positioning it as a top choice for real-time image encryption applications. Looking ahead, this methodology holds promise for extending encryption to diverse data formats, including audio and video files not only related to medicine realm but also in other fields.

DECLARATION

CONFLICT OF INTEREST

The contributors guarantee that they do not have any conflict of interest.

FUNDING INFORMATION

The authors have received no funding assistance for the implementation of the proposed method.

DATA AVAILABILITY

The data (medical images) on which the proposed technique was implemented on are available from the corresponding author, upon reasonable request. The other standard images used for further comparisons were obtained from [26]. The article and the supplementary files contain all the generated and analysed data that led to the conclusion of the proposed method.

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 multi-dimensional 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.

[11] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, "Construction of S-boxes using different maps over elliptic curves for image encryption," *IEEE Access*, vol. 9, pp. 157106–157123, 2021.

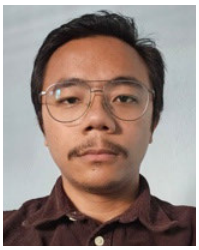
[12] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Arch. Computat. Methods Eng.*, vol. 27, pp. 15-43, 2020.

[13] Z. Bashir, M. A. Malik, M. Hussain, and N. Iqbal, "Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol," *Multimedia Tools Appl.*, vol. 81, no. 3, pp. 3867–3897, 2022.

[14] U. Hayat, I. Ullah, N. A. Azam, and S. Azhar, "A novel image encryption scheme based on elliptic curves over finite rings," *Entropy*, vol. 24, no. 5, p. 571, 2022.

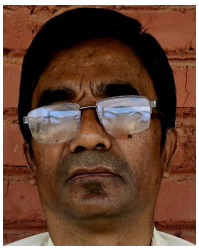
[15] A. M. Abbas, A. A. Alharbi, and S. Ibrahim, "A novel parallelizable chaotic image encryption scheme based on elliptic curves," *IEEE Access*, vol. 9, pp. 54978–54991, 2021.

[16] S. Yin, J. Liu, and L. Teng, "Improved elliptic curve cryptography with homomorphic encryption for medical image encryption," *Int. J. Netw. Secur.*, vol. 22, no. 3, pp. 419–424, 2020.
[17] M. Blum and S. Goldwasser, "An efficient probabilistic public-key encryption scheme which hides all partial information," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1984, pp. 289–299.
[18] J. S. Muthu and P. Murali, "A new chaotic map with large chaotic band for a secured image cryptosystem," *Optik*, vol. 242, Sep. 2021, Art. no. 167300.
[19] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8629–8652, Apr. 2018.
[20] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimedia Tools Appl.*, vol. 79, nos. 33–34, pp. 24993–25022, Sep. 2020.
[21] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13841–13864, Apr. 2021.
[22] K. M. Singh, L. D. Singh, and T. Tuithung, "Improvement of image transmission using chaotic system and elliptic curve cryptography," *Multimedia Tools Appl.*, vol. 82, no. 1, pp. 1149–1170, Jan. 2023.
[23] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018.
[24] J. Wu, Z. Liu, J. Wang, L. Hu, and S. Liu, "A compact image encryption system based on Arnold transformation," *Multimedia Tools Appl.*, vol. 80, pp. 2647–2661, Jan. 2021.
[25] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2020.
[26] *The USC-SIPI Image Database*. Accessed: Jan. 25, 2024. [Online]. Available: http://sipi.usc.edu/database/



TUTU RAJA NINGTHOUKHONGJAM received the B.Eng. degree from the Sir M. Visvesvaraya Institute of Technology, Bengaluru, India, in 2017, and the M.Tech. degree in computer science and engineering from the National Institute of Technology Manipur, in 2019, where he is currently pursuing the Ph.D. degree in computer science and engineering. His research interests include cryptography and image security.

SURSITA DEVI HEISNAM received the B.Eng. degree in computer science and engineering from the Alva's Institute of Engineering and Technology, VTU, in 2019, and the M.Tech. degree in computer science and technology from the National Institute of Technology Manipur, India, in 2021, where she is currently pursuing the Ph.D. degree in digital signatures



MANGLEM SINGH KHUMANTHEM is currently a Professor with the National Institute of Technology Manipur, India. He is also a distinguished academic in computer science and engineering. With a profound expertise in digital image and video processing, digital watermarking, information hiding, cryptography, hashing functions, and cyber forensics, he has contributed significantly to these domains. Known for his prolific publication record, his work has been featured in numerous reputed international journals. His research explores innovative solutions for securing digital information, with a focus on image and video processing.