International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 14s, 2025
https://www.theaspd.com/ijes.php

Image Encryption Using Baker's Map, Ecc With Alphanumeric Flip Transformation

Rupesh Malla[1*], Pankaj Sonawane[2]

[1*]Department of Computer Engineering, D.J. Sanghvi, College of Engineering Mumbai, India.
Email: mallarupesh491@gmail.com
[2]Department of Computer Engineering, D.J. Sanghvi College of Engineering Mumbai, India.
Email: pankaj.sonawane@djsce.ac.in.
*Corresponding author: Rupesh Malla
*Email: mallarupesh491@gmail.com

Abstract *– In the world with the rapid expansion of digital communication, the security of visual data has become a critical concern forcing robust encryption mechanisms that ensures confidentiality, integrity, unauthorized access, and resistance to attacks. In this paper, we introduce a novel idea of hybrid image encryption and decryption framework that creates an alphanumeric text which can be used in QR codes, with Base64 and as metadata etc. It uses*
Baker's Map which ensures chaotic pixel scrambling, while ECC key generation extracts cryptographic keys directly from encrypted image pixels from baker's map. Then it produces private key and public key from base point in ECC. Alphanumeric Flip Transformation takes private and public key elements enhancing obfuscation and resistance to attacks. Experimental results show Maximum entropy of , minimal pixel correlation, and improved efficiency compared to existing chaotic-ECC approaches, making the scheme both lightweight and secure for visual data protection

Keywords *– Image Encryption, Chaotic Map (Baker's Map), Cryptography, Security, Elliptic curve cryptography (ECC), Alphanumeric Flip Transformation, Secure Communication, Privacy- Preserving Encryption.*

I. INTRODUCTION

The exponential growth of digital communication has caused an unprecedented increase in the transmission and the storage of visual data across various platforms[12]. With the increasing reliance on digital communication securing multimedia data particularly images have become a fundamental requirement in a various number of fields, including medical imaging, secure communication, and cloud storage. Traditional encryption methods like Advanced Encryption standard (AES) and RivestShamir-Adleman (RSA) [13] provides the strongest security but often suffers from making them unsuitable for real-time encryption images in limited resource environments [14].

To overcome these limitations, many researchers and scholars have explored chaotic maps and elliptic curve cryptography (ECC) to develop lightweight but extremely secure encryption mechanisms.

Chaotic maps, like Baker's Map, Arnold's Cat Map, and Logistic Map, have gained significant attention for image encryption due to their high sensitivity for initial conditions, making them ideal for generating random transformations that ensure strong diffusion and confusion properties [15].

Among these, Baker's Map has demonstrated superior effectiveness in pixel scrambling, achieving high number of entropy and low number of correlations between adjacent pixels, which significantly enhances defense against statistical and differential attacks Kumar et al. (2024)[1][14]. However, while chaotic encryption provides strong diffusion properties, it lacks inherent cryptographic strength for key management, making it vulnerable to brute-force and key-recovery attacks[16]. Elliptic Curve Cryptography (ECC) is a lightweight public-key cryptosystem that offers high level of security with smaller key sizes compared to RSA making it highly suitable for secure image encryption in computationally controlled environments Khalid et al. (2022)[2].

Conventional ECC-based encryption systems mainly focus on key exchange mechanisms, which requires additional key management infrastructure. In this study they have integrated ECC with chaotic systems to strengthen image encryption, such as the work in Parida et al. (2021)[3], which combines the Arnold's Cat Map with ECC to enhance security. To overcome these limitations, this paper proposes a hybrid image encryption framework that integrates Baker's Map, ECC- based key generation, and a novel Alphanumeric Flip

Transformation[17]. The Baker's Map is applied to the image to achieve chaotic pixel scrambling, ensuring high diffusion. Instead of relying on external key distribution, ECC keys are directly generated from the encrypted image pixels using SHA- 256 hashing, binding cryptographic security to the visual data itself. To further enhance key obfuscation and storage security, we introduce the Alphanumeric Flip Transformation, which interleaves ECC private and public key components into a structured alphanumeric format, making unauthorized key reconstruction significantly more difficult.

II. LITERATURE REVIEW

Kumar, Sanjay, and Deepmala Sharma in [1] presents a new image encryption system that combines Arnold's Cat Map for pixel scrambling, elliptic curve cryptography (ECC) for secure encryption, and a genetic algorithm (GA) for optimizing key generation[18]. This approach ensures high security, efficiency, and robustness against attacks by introducing chaos, optimizing encryption keys, and reducing computational overhead, making it ideal for secure image transfer and storage.

The paper proposed by Khalid, Ijaz, et al [2] proposes a secure image encryption method using Elliptic Curve Cryptography (ECC) and symmetric key encryption. It combines ECC-based Diffie-Hellman key exchange with SHA-256 hashing to generate encryption and authentication keys. The encryption process includes affine power affine transformations for confusion and elliptic curve-based pseudorandom sequences for diffusion, ensuring strong resistance to various attacks, including differential and statistical attacks. The scheme offers high security, efficiency, and a large key space, making it ideal for protecting sensitive images transmitted over insecure networks.

Rashmi, P., and M. C. Supriya [3] optimized image encryption method combining Continuous Raster Scan, Henon Chaotic Map, and Chebyshev Chaotic Map. The process involves scrambling image pixels, permuting blocks with chaotic maps, and using a secret key-based random matrix for additional security. A bitwise XOR operation is applied to produce the encrypted image. The method is tested on color images, showing improved security through uniform histograms, low correlation between pixels, and resistance to differential attacks. The encryption algorithm is efficient and secure, with potential applications in secure image communication.

Lin, Chia-Hung, et al. [4] presents a novel approach to securing medical images through an intelligent symmetric cryptography method that integrates chaotic maps and quantum-based key generation. This technique generates complex cipher codes using a hybrid sine-power chaotic map and logistic map, enhancing security against unauthorized access. The encryption and decryption processes are facilitated by grey relational analysis (GRA) models, which allow for rapid retraining of cipher codes. The methodology was validated using a chest X-ray database, achieving a structural similarity index measurement (SSIM) of 0.95 or higher, indicating reliable and lossless decryption. Overall, the proposed system effectively protects sensitive medical data from eavesdropping while maintaining image integrity for diagnostic use.

Hafsa, Amal, et al. [5] proposes a hybrid cryptographic approach for securing medical images, combining Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC). They introduce a modified AES (MAES) that enhances encryption speed by simplifying operations, specifically by eliminating the mix-columns transformation and replacing it with a more efficient permutation method. Additionally, an optimized ECC architecture is presented, which uses fewer multipliers to improve processing efficiency while maintaining security for the symmetric session key. This system is implemented on an FPGA platform, demonstrating significant reductions in execution time, making it suitable for real-time applications in embedded systems. The results indicate that the proposed method effectively balances security and performance, addressing the challenges of existing encryption techniques in medical image transmission.

The paper in [6] presents a robust image encryption and authentication model combining Elliptic Curve Cryptography (ECC) and multidimensional chaotic maps to secure grayscale and color images. Using Elliptic Curve Diffie-Hellman (ECDH) key exchange for secure key generation and Arnold Cat maps (3D and 4D) for pixel scrambling, the model ensures high encryption quality. It incorporates improved ElGamal encoding for encryption and a digital signature for verifying image authenticity. The proposed method achieves strong security with high entropy (≈7.9993), low correlation, and strong resistance to statistical, differential, known-plaintext, and chosen-plaintext attacks, while maintaining efficiency with minimal computational cost. Experimental results confirm that the model generates secure cipher images with a high degree of randomness and performs well against occlusion and intruder attacks.

Meanwhile in [7] proposes a hybrid image encryption method that combines chaotic maps and a genetic algorithm for enhanced security. The encryption process involves three key phases: confusion, where a Chen chaotic map scrambles image pixels; diffusion, where a Logistic-Sine chaotic map alters pixel intensity; and optimization, where a genetic algorithm minimizes pixel correlation in the encrypted image. This approach ensures a large key space, high sensitivity to key changes, and robustness against statistical, differential, noise, and data loss attacks. Simulation results demonstrate the method's effectiveness, producing encrypted images with uniform histograms, near-zero-pixel correlation, high entropy, and strong resilience against security attacks. The authors suggest that the proposed method provides a secure and efficient encryption scheme for image data, with potential improvements through further exploration of chaotic systems and optimization algorithms.
In this [8] proposes a dual system for securing multimedia data, using an improved chaotic logistic map. The chaotic system, known for its randomness and sensitivity to initial conditions, enhances image encryption and watermarking. For encryption, the method randomizes pixel values through image rotation, substitution, and chaotic sequences to produce a noise-like, unreadable image. The watermarking scheme embeds secret data into an image by altering its least significant bits (LSBs), guided by the chaotic map, ensuring imperceptibility. Simulations show that the system is robust against attacks, with strong security keys, high resistance to differential attacks (as indicated by NPCR and UACI values), and effective statistical performance (entropy and PSNR). The results demonstrate the system's security, efficiency, and suitability for multimedia protection.
And paper in [9] gives a novel image encryption method that combines Elliptic Curve ElGamal (ECElGamal) encryption and chaotic systems to address key management issues in symmetric encryption while enhancing security. The process begins by generating initial values using SHA-512 hashing to create chaotic sequences, followed by a crossover permutation to scramble the image pixels. The scrambled image is then encrypted using the EC-ElGamal cryptosystem, which leverages elliptic curve cryptography for efficient, asymmetric encryption. Finally, a diffusion process based on the chaos in game and DNA sequence operations is applied to further randomize the pixel values. The proposed method demonstrates high security, including resistance to statistical, chosen- plaintext, and brute force attacks, with a strong avalanche effect and uniform histogram distribution. The system offers efficient encryption while solving key distribution problems, making it suitable for secure image transmission in fields like medical imaging and communications.
In [10] this paper presents a new chaos- based parallel image encryption algorithm that improves both security and performance. Traditional encryption methods like AES and RSA are not efficient for large datasets like images, prompting the use an chaotic systems due to its sensitivity to initial conditions, which ensures high randomness. The proposed algorithm incorporates a new Random Number Generator (RNG) and uses parallel computing to speed up the encryption process by dividing the workload across multiple CPU cores. This approach increases the key space, making the encryption more secure. Extensive tests, including time analysis, correlation, differential cryptanalysis, and entropy evaluations, demonstrate that the parallel algorithm is 9 times faster than [14] non-parallel methods, with enhanced security features such as strong resistance to attacks and a significantly big key space, making it well-suited for real-time applications involving large multimedia data[24].

III. BACKGROUND

3.1. Baker's Map for Chaotic Pixel Scrambling

Baker's Map is one of the chaotic transformations originating from dynamical systems theory, often described as a process like "kneading dough," where an initial structure is stretched, folded, and shuffled iteratively. This process ensures a high level of diffusion in image encryption, [1] meaning a small changes in input can lead to unpredictable results, making it resistant to differential and statistical attacks. The standard Baker map is defined on the unit square $U=[0,1]\times[0,1]$ by the mathematical relations.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 14s, 2025
https://www.theaspd.com/ijes.php

The folded baker's map is a two-dimensional

[29][30][31]

$$B(x,y) = \begin{cases} (2x, \frac{y}{2}), & 0 \le x \le \frac{1}{2} \\ (2x-1, \frac{y+1}{2}), & \frac{1}{2} \le x \le 1. \end{cases}$$

: (1)

For image encryption it iteratively rearranges pixel positions disrupting the spatial correlation between neighboring pixels. It works as the input image is divided into two equal halves (left and right). Each half is stretched and rearranged non-linearly according to the baker's Map function. Iterative transformation is repeated multiple times to ensure strong pixel diffusion. The more iteration applied higher the diffusion and more security. The original image can be recovered by using the inverse operation as the Baker's Map is deterministic transformation[23].

3.2. Elliptic Curve Cryptography (ECC) for Key Generation.

Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic system that offers the same level of security in traditional RSA encryption but with much smaller key sizes. ECC operates over elliptic curves, where encryption and decryption rely on the Elliptic Curve Discrete Logarithm Problem (ECDLP) a problem that is computationally infeasible to reverse without knowing the private key.

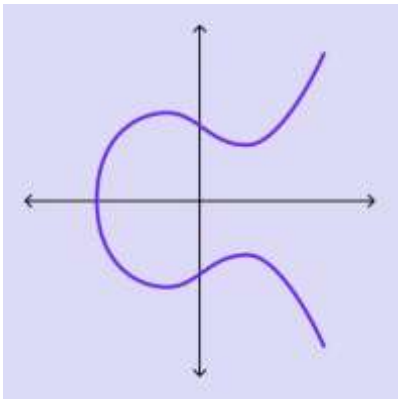


Fig 1: curve diagram of ECC

The general form of an elliptic curve equation is: [11]

$$y^2=x^3+ax+b \quad (2)$$

where:

- a, b are constants defining the curve in this equation.
- x,y represents points on the curve.

ECC instead of using a randomly generated ECC key in this paper the keys derived directly from the encrypted image pixels. In this process the grayscale intensity values of pixels are converted into a 1D array. ECC is widely in used for secure communications, digital signatures, and key exchange because it provides high level of security with the minimum computational process. This pixel data serves as a deterministic input for cryptographic hashing. The pixel data is hashed using SHA- 256 algorithm producing a 256-bit hash. The fist 32 bytes of the hash are extracted to serve as the private ECC key. Using NIST P-256 (a standard elliptic curve) an ECC private key is than generated corresponding public key is derived by multiplying private key with the elliptic curve generator point. The ECC key directly depends on image content making it unique for each image and as key is derived from the encrypted image external storage for key is not needed reducing exposure risks.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 14s, 2025
https://www.theaspd.com/ijes.php

3.3. Alphanumeric Flip transformation

While ECC provides strong security, key still exposure remains a significant risk in cryptographic systems. Attackers who intercept an ECC private key can decrypt the data. To increase key complexity and reduce predictability, this research introduces Alphanumeric Flip Transformation—a novel approach for obfuscating the ECC private key. The Alphanumeric Flip
Transformation interleaves private and public key values making key reconstruction difficult. The ECC private key and public key are converted to hex format (since ECC keys are binary values). The hex characters of the private and public keys are interleaved to for a structed alphanumeric sequence.

Example:

- Private Key (Hex): a1b2c3d4e5f6...
- Public Key (Hex): 9f8e7d6c5b4a...
- Alphanumeric Flip
- Output: 9a1f8b2e7c3d6d5c4b4a...

If one key is longer its remaining part is appended at the end. This makes the final alphanumeric sequence unpredictable even if an attacker gains partial knowledge of either key. This prevents direct retrieval of ECC private keys increasing resilience against key extraction attacks. Reducing key predictability making it more difficult for attackers to reconstruct the key and enhances storage security since an attacker who intercepts the alphanumeric sequence cannot easily separate private and public key elements.

Currently there are many algorithms which can convert private and public key to Alphanumeric texts like Base64 Encoding, Hexadecimal encoding, AES Encryption, RSA Encryption, SHA-256 Hash. But the Alphanumeric Flip Transformation (AFT) offers a novel approach to key obfuscation and security distinguishing itself from existing encoding and encryption techniques. Unlike Base64 and Hex encoding, which only convert data into readable formats without enhancing security, AFT interleaves private and public key characters, preventing direct key extraction and making pattern-based attacks significantly harder. Unlike AES and RSA encryption, which rely on external secret keys and introduce computational overhead, AFT secures keys without additional cryptographic operations, making it lightweight and efficient. Compared to one-way hashing like SHA-256, which is irreversible, AFT remains reversible while maintaining strong key hidden inside it. This type of transformation disrupts key structures, prevents statistical attacks, and ensures secure key storage, making it a good solution for real-time encryption and privacy- preserving applications.

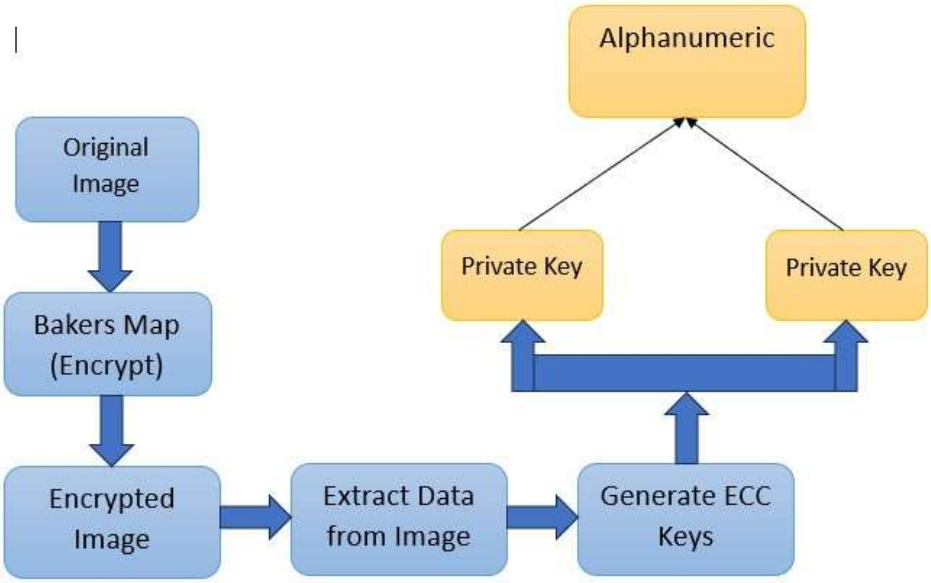


Fig 2: Architecture Design

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 14s, 2025
https://www.theaspd.com/ijes.php

IV. METHODOLOGY

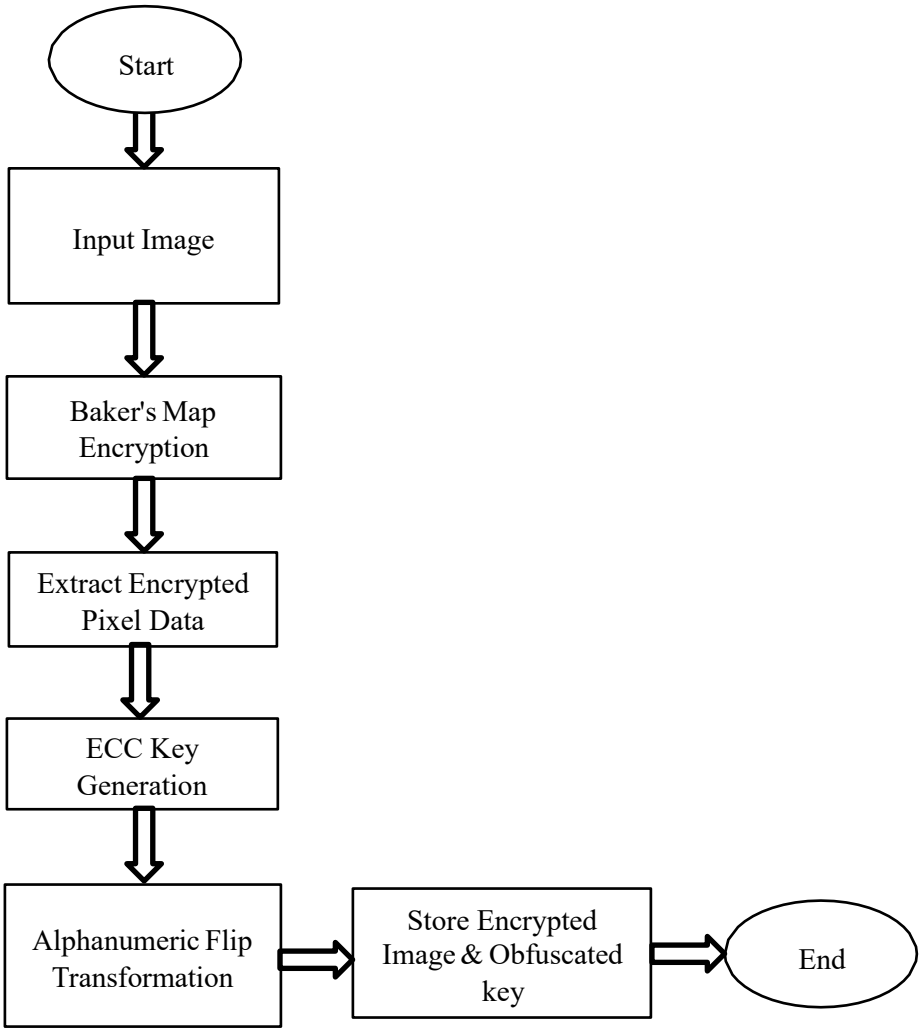


Fig 3: Flow Diagram of Encryption Algorithm

The proposed encryption framework integrates Baker's Map, Elliptic Curve Cryptography (ECC), and the Alphanumeric Flip Transformation (AFT) to get more secure, lightweight, and efficient image encryption. This methodology ensures high diffusion, strong key management, and resistance against cryptographic attacks, making that suitable for real-time secure communication and data storage applications[22].

The encryption process in this system follows a structured workflow, ensuring strong security properties while maintaining computational efficiency.

1. Image Preprocessing The input image is read by system and converted to RGB format to maintain compatibility. Image dimensions are extracted and prepared for chaotic transformation.
2. Baker's Map-Based Image Encryption The image undergoes multiple iterations of Baker's Map transformation, scrambling pixel positions chaotically. The transformation ensures that even if did small changes in input can cause significant differences in encrypted image[21]. This also ensures chaotic pixel rearrangement reducing statistical correlation and enhancing diffusion. The encrypted image is stored as an intermediate output.
3. ECC Key Generation from Image Pixels In this ECC helps to directly derives cryptographic keys from image data instead of relying on external key storage. The grayscale pixel values of the encrypted image are extracted and flattened into a 1D array. A SHA256 hash is applied to this pixel data, producing a 256-bit cryptographic

digest. The first 32 bytes of the hash are used as the ECC private key, while the corresponding public key is derived using elliptic curve multiplication [20].

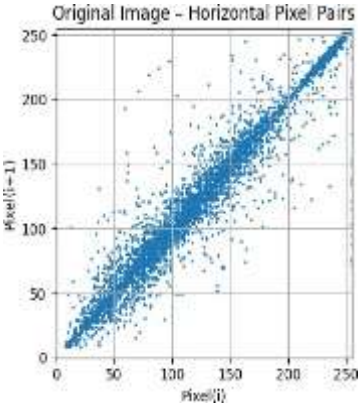
4. Alphanumeric Flip Transformation for Key Obfuscation the ECC private and public keys (converted to hex format) are interleaved character by character, forming a structured alphanumeric sequence. If one key is longer, the remaining characters are appended at the end. This obfuscated key representation prevents direct key extraction, increasing security.
5. Storing Encrypted Image and Keys Input Image Baker's Map Encryption Extract Encrypted Pixel Data ECC Key Generation Alphanumeric Flip Transformation End Store Encrypted Image & Obfuscated key The encrypted image is saved for transmission or storage. The obscured ECC key (AFT output) is been stored securely by ensuring safe key management without relying on external storage in the system.

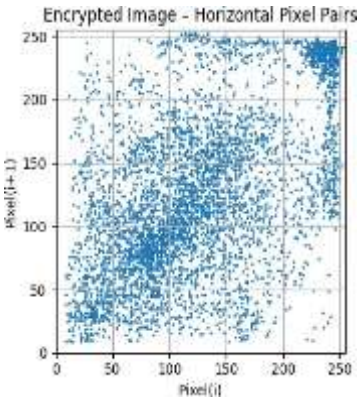
This methodology integrates the chaotic encryption, lightweight cryptographic key generation, and novel obfuscation technique to get a more secure and efficient image encryption system. This architecture ensures high level of security, resistance key-recovery attacks and computational efficiency making it suitable for secure communication and privacy storage applications.

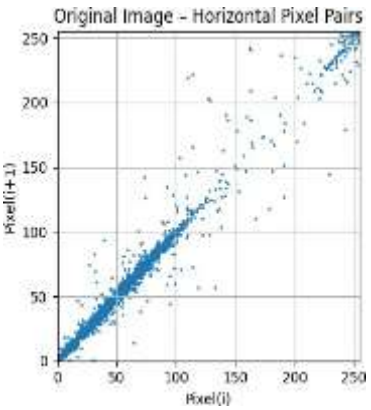
V. RESULT

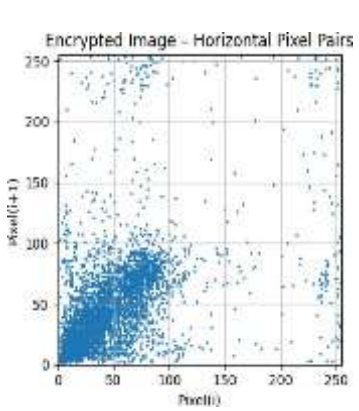
Correlation Analysis:

Correlation analysis is one of the most effective methods for determining the relationship between neighboring pixel values in an image [25]. By conducting this correlation analysis between the plain image and the encrypted image, we can evaluate the relationship between the pixel values in both images. This analysis helps us to understand how the encryption process affects the correlation patterns of pixel values. Here is correlation analysis of some images based on my proposed algorithm.









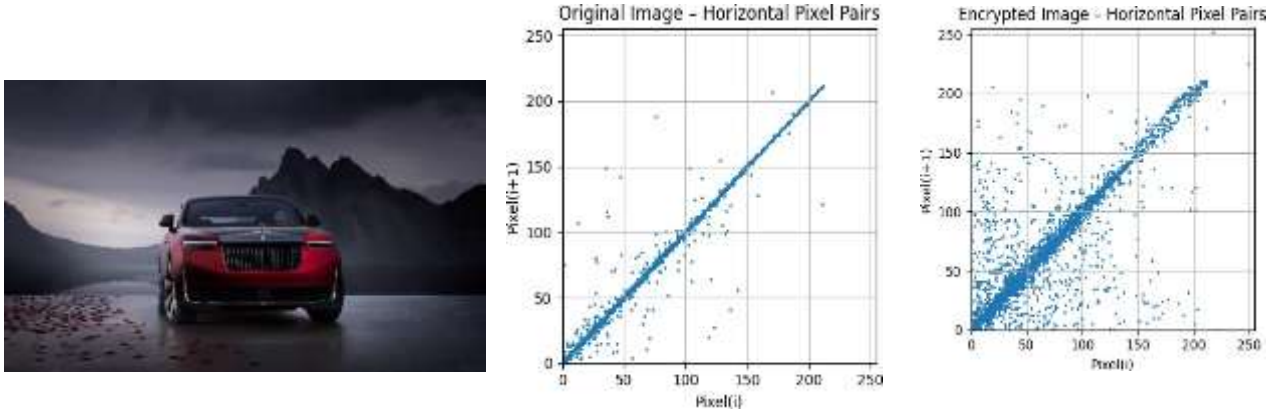


Fig 4: Correlation Analysis of 3 Images with Original image, Analysis of Original image and analysis of encrypted images.

The result confirms that it's very effective of the proposed image encryption scheme in reducing the correlation between neighboring pixels. But some images it differs.

Entropy Analysis:

The Entropy analysis is used to measure the level of randomness and information content found in both the original and encrypted images using the proposed image encryption system. This Equation calculates the information entropy [26][27].

$$H(s) = \sum_{j=0}^{j=2^N-1} P(s_j) log_2(\frac{1}{P(s_j)}) \quad (3)$$

In the provided context, N signifies the quality of bits needed to represent the symbol sj , while P(sj) represents the likelihood of the symbol sj occurring. We used entropy analysis to understand the level of randomness and information in both original input image and encrypted output image. This entropy level is calculated using Shannon's theory of information. An ideal encryption system/algorithm should produce an encrypted image with an entropy value of 8 or closer to 8[28]. We found that the entropy values of the encrypted images produced by our proposed scheme were quite standard than those of the encryption techniques currently used, indicating a good level of randomness and improved security. My entropy of the images are average around (6.9). These results demonstrate the efficiency of our encryption scheme in introducing greater uncertainty and protecting image data from unauthorized access.

	Red Shirt	Baboon	Old Car	Pepper
OI	6.9904	6.6187	7.4554	6.9511
EI	6.9904	6.6187	7.4554	6.9511

Table 1: Entropy of Original images and their Encrypted image

Key space analysis:

Key space analysis examines the size and intricacy of the encryption key space used in the proposed encryption algorithm. A larger key space enhances and helps in security by rendering it exceedingly it will be difficult for attackers to guess or exhaustively search for the key. In our proposed algorithm, the key space is 2^{256}, which is larger. A large key space exponentially expands the number of potential key combinations, making it computationally infeasible to try all combinations within a given time frame. These findings emphasize that how effective is the proposed encryption method in creating a strong and secure key space, ensuring the integrity and confidentiality of the encrypted image data.

Key sensitivity analysis:
To evaluate the sensitivity of the encryption key and its impact on the encrypted image, we conducted key analysis experiments. The key analysis involved systematically varying the encryption key while keeping all other parameters constant. During the key analysis, we selected a set of representative images and encrypted them using the proposed encryption scheme. We then generated multiple cipher images by modifying specific bits or components of the encryption key. By comparing the resulting cipher images, we assessed the effect of key variations on the encryption process. We analyzed the changes in the encrypted image quality, security, and resistance against decryption attempts. The key analysis revealed that even slight modifications in the encryption key led to significant changes in the cipher image. This demonstrated the high sensitivity of the encryption key and its crucial role in ensuring the security and confidentiality of the encrypted data.

Computational Complexity:
The time complexity of encryption algorithms is significant, especially in scenarios involving realtime internet tasks and the processing of extensive data sets.

Text Image	Proposed	Hu et al. (2017)	Wang and Liu (2017)	Liu and Wang (2012)	Chai et al. (2019)	Zhan et al. (2017)	Sanjay et al. (2024)
Baboon	0.145067	14.9134	15.8617	71.3306	19.7477	38.0776	0.8692
Lena	0.045512	14.8401	15.8259	71.7947	10.8232	38.5336	0.8572
Peppers	0.023992	14.6393	13.2887	71.6727	10.6869	36.9910	0.8524
Cameraman	0.045550	15.2032	13.4003	71.6566	10.7977	36.7060	0.8567

Table 2: Time Complexity in Encryption Process

Text Image	Proposed	Hu et al. (2017)	Wang and Liu (2017)	Liu and Wang (2012)	Chai et al. (2019)	Zhan et al. (2017)	Sanjay et al. (2024)
Baboon	0.145067	14.9678	13.3824	71.2461	10.7146	36.5774	0.8692
Lena	0.024071	14.9266	13.3493	72.0903	10.6952	37.2344	0.8572
Peppers	0.012283	14.7637	13.2887	71.6727	10.6869	36.9910	0.8524
Cameraman	0.023896	15.2032	13.4003	71.6566	10.7977	36.7060	0.8567

Table 3: Time Complexity in Decryption Process

This experiment was done with hardware of 8GB RAM and 2.4 GHz. The experiment was done with four images “Baboon”, “Lena”, “Peppers”, and “Cameraman”. As can be seen in this table.

VI. CONCLUSION

This study has introduced a brand-new type of novel system which is hybrid picture encryption system that incorporates Baker's Map, the proposed Alphanumeric Flip Transformation and Elliptic Curve Cryptography (ECC) provide lightweight cryptographic security, safe key management, and high diffusion. By directly obtaining ECC keys from pixels in the picture, as opposed to conventional techniques that depend on external key storage, this method improves the security and gets rid of key exchange issues which are common in current version of systems. By merging the private and the public key structures in one Alphanumeric Flip Transformation it improves the security even more and makes it far more difficult for unauthorized parties to reconstruct keys. This framework maintains computational efficiency appropriate for real-time encryption and secure data transmission while achieving greater resilience against brute force, statistical, and pattern recognition attacks in comparison to current chaotic encryption techniques, ECC based image security models, and hybrid approaches[19]. The experimental method’s results confirm that the method’s robust security, minimal correlation, and strong encryption quality, making it a promising solution for privacy in applications to secure image communication and storage of it.

REFERENCES

1. Kumar, Sanjay, and Deepmala Sharma. "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm." Artificial Intelligence Review 57.4 (2024): 87.
2. Khalid, Ijaz, Tariq Shah, Sayed M. Eldin, Dawood Shah, Muhammad Asif, and Imran Saddique. "An integrated image encryption scheme based on elliptic curve." IEEE Access 11 (2022): 5483-5501. 3. Rashmi, P., and M. C. Supriya. "Optimized Chaotic encrypted image based on continuous raster scan method." Global Transitions Proceedings 2.2 (2021): 589- 593.
4. Lin, Chia-Hung, et al. "Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity." IEEE Access 9 (2021): 118624-118639.
5. Hafsa, Amal, et al. "Image encryption method based on improved ECC and modified AES algorithm." Multimedia Tools and Applications 80 (2021): 19769-19801.
6. Parida, Priyansi, et al. "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps." IEEE Access 9 (2021): 76191- 76204.
7. Ghazvini, Mahdieh, Mojdeh Mirzadi, and Negin Parvar. "A modified method for image encryption based on chaotic map and genetic algorithm." Multimedia Tools and Applications 79.37 (2020): 26927-26950.
8. Attaullah, Tariq Shah, and Sajjad Shaukat Jamal. "An improved chaotic cryptosystem for image encryption and digital watermarking. " Wireless personal communications 110.3 (2020): 1429-1442.
9. Luo, Yuling, et al. "An image encryption method based on elliptic curve elgamal encryption and chaotic systems." IEEE Access 7 (2019): 38507- 38522.
10. Çavuşoğlu, Ünal, and Sezgin Kaçar. "A novel parallel image encryption algorithm based on chaos." Cluster Computing 22 (2019): 1211-1223.
11. Yan, Yuhan. (2022). The Overview of Elliptic Curve Cryptography (ECC). Journal of Physics: Conference Series. 2386. 012019. https://10.1088/1742- 6596/2386/1/012019 .
12. Hussain, I., Shah, T., Gondal, M.A. et al. Efficient method for designing chaotic Sboxes based on generalized Baker's map and TDERC chaotic sequence. Nonlinear Dyn 74, 271–275 (2013). https://doi.org/10. 1007/s11071-013-0963-z.
13. Bin Zhu, Edina, Guofei Gu, Shipeng Li, Irvine eta. al. Digital rights management system. 2009. https://www.freepatentsonline.com/75942 75.html.
14. Kumar, S., Sharma, D. Image scrambling encryption using chaotic map and genetic algorithm: a hybrid approach for enhanced security. Nonlinear Dyn 112, 12537–12564 (2024). https://doi.org/10.1007/s11071-024- 09670-0.
15. Adil Waheed, Fazli Subhan, Mazliham Mohd Suud, Muhammad Mansoor Alam, Sajjad Haider, Design and optimization of nonlinear component of block cipher: Applications to multimedia security, Ain Shams Engineering Journal, Volume 15, Issue 3, 2024, 102507, ISSN 2090-4479, https://doi.org/ 10.1016/j.asej. 2023.102507 .
16. Kartikey Pandey, Deepmala Sharma, Novel image encryption algorithm utilizing hybrid chaotic maps and Elliptic Curve Cryptography with genetic algorithm, Journal of Information Security and Applications, Volume 89, 2025, 103995, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2025.103995 . 17. SHAKIR, Huda R.; MEHDI, Sadiq A.; HATTAB, Anwar A. A new fourdimensional hyper-chaotic system for image encryption. International Journal of Electrical and Computer Engineering (IJECE), [S.l.], v. 13, n. 2, p. 1744-1756, apr. 2023. ISSN 2722-2578. Available at: doi: http://doi.org/10.11591/ijece.v13i2.pp1744- 1756.
18. Arman Sykot Md Shawmoon Azad Wahida Rahman Tanha BM Monjur Morshed Syed Emad Uddin Shubha M.R.C. Mahdy et al. https://arxiv.org/html/2408.06964v1.
19. Guanrong Chen, Yaobin Mao, Charles K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals, Volume 21, Issue 3, 2004, ISSN 0960-0779, https://doi.org/ 10.1016/j.chaos.2003.12.02 .
20. Jebrane, J.; Chhaybi, A.; Lazaar, S.; Nitaj, A. Elliptic Curve Cryptography with Machine Learning. Cryptography 2025, 9, 3. https://doi.org/10.3390/cryptography90100 03 .
21. Arman Sykot, Md Shawmoon Azad, Wahida Rahman Tanha, B.M. Monjur Morshed, Syed Emad Uddin Shubha, M.R.C. Mahdy, Multi-layered security system: Integrating quantum key distribution with classical cryptography to enhance steganographic security, Alexandria Engineering Journal, Volume 121, 2025, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2025.02.056 .
22. Janakiraman, S., R, V.R., Sivaraman, R. et al. Integrity verified lightweight ciphering for secure medical image sharing between embedded SoCs. Sci Rep 15, 7465 (2025). https://doi.org/10.1038/s41598-025-91431- z.
23. Anlin Wang, Chuan Shen, Junqiao Pan, Cheng Zhang, Hong Cheng, and Sui Wei "Research on multiple-image encryption method using modified Gerchberg–Saxton algorithm and chaotic systems," Optical Engineering 62(9), 098103 (21 September 2023). https://doi.org/10.1117/1.OE.62.9.09 8103 24. Benyahia, K., Khobzaoui, A. & Benbakreti, S. Hybrid image encryption: leveraging DNA sequencing and Lorenz chaotic dynamics for enhanced security. Cluster Comput 28, 218 (2025). https://doi.org/10.1007/s10586-024-04948- 9.

25. Enayatifar R, Abdullah AH, Isnin IF, Altameem A, Lee M (2017) Image encryption using a synchronous permutation-difusion technique. Opt Lasers Eng 90:146–154. https://doi.org/10.1016/j.optlaseng.2016. 10.006 .
26. Abdullah AH, Enayatifar R, Lee M (2012) A hybrid genetic algorithm and chaotic function model for image encryption. AEU-Int J Electron Commun 66(10):806–816. https://doi.org/10.1016/j.aeue.2012.01. 015
27. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36. https://doi.org/10.1016/j.optlaseng.201 6.03.019
28. Xu L, Gou X, Li Z, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based difusion. Opt Lasers Eng 91:41–52. https://doi.org/10.1016/j.optlaseng.201 6.10. 012.
29. Karawia, Abdelrahman & Fouda, Y.. (2022). Image encryption via a 2-D Logistic-Baker map and fractional discrete Meixner moments. 10.21203/rs.3.rs-2252710/v1
30. C. Li and K. Tan, "The Graph Structure of Baker's Maps Implemented on a Computer," in IEEE Transactions on Computers, vol. 74, no. 5, pp. 1524-1537, May 2025, doi: 10.1109/TC.2025.3533094.
31. Tarlok Singh, Pammy Manchanda, "An Efficient Image Encryption Technique using Discretized Baker Map in Shearlet Domain," in International Journal of Computer Sciences and Engineering, vol. 6, issue-7, July 2018.