IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

IMPROVEMENT OF IMAGE TRANSMISSION USING CHAOTIC SYSTEM AND ELLIPTIC CURVE CRYPTOGRAPHY

[1]Prasanna Nandini Kandula

MCA

Sir C R Reddy College Of Engineering - Near, Railway Gate, Vatluru, Eluru, Andhra Pradesh 534007

[2]Dr. G.Nirmala M.Tech., Ph.D, Professor

Sir C R Reddy College Of Engineering - Near, Railway Gate, Vatluru, Eluru, Andhra Pradesh 534007

ABSTRACT

Secure and reliable image transmission is critical in modern communication systems. This project presents a hybrid encryption scheme that integrates a chaotic system with Elliptic Curve Cryptography (ECC) to enhance the security and quality of image transmission. The proposed method utilizes chaotic maps to introduce high randomness, which is further reinforced by ECC-based key generation via the Diffie-Hellman algorithm. XOR-based encryption with pixel grouping is applied for increased resistance against statistical attacks. The system's GUI facilitates user interaction for uploading images, generating secure keys, encrypting, decrypting, and comparing results. Experimental outcomes demonstrate that the proposed approach significantly improves image quality after decryption, as evidenced by higher PSNR and SSIM values compared to existing techniques. Visual comparisons also reveal a substantial improvement in preserving the original image content, making this method highly effective for secure image transmission.

1. INTRODUCTION

1.1 Background and Motivation

In today's digital era, secure image transmission has become a critical component in fields like telemedicine, military communication, online identity verification, and multimedia broadcasting. Traditional encryption methods, though effective, are increasingly susceptible to cyber threats due to advancements in computational power and cryptanalysis techniques. Therefore, the need for robust, lightweight, and highly secure encryption algorithms has never been more pressing.

This project is motivated by the potential of combining two powerful techniques—**chaotic systems** and **elliptic curve cryptography (ECC)**—to enhance the reliability and security of image data transmission. Chaotic systems offer sensitivity to initial conditions and pseudo-random behavior ideal for encryption, while ECC ensures secure key exchange with lower computational overhead compared to traditional RSA.

1.2 Role of Chaotic Systems and ECC in Secure Image Transmission

Chaotic systems play a pivotal role in ensuring pixel-level diffusion and confusion during image encryption. Their non-linear, deterministic nature

ISSN 2347–3657

Volume 13, Issue 2, 2025

introduces high unpredictability, making brute-force and statistical attacks difficult. In this work, chaotic maps are used for generating pseudo-random sequences that determine the encryption pattern over image pixels.

Elliptic Curve Cryptography is employed to generate secure key pairs and share encryption keys using the Diffie-Hellman protocol. ECC offers stronger security per bit compared to RSA, allowing for faster computation and smaller key sizes, which is especially important for real-time or resource-constrained environments.

The integration of both methods allows for:

Generation of strong secret keys. Efficient pixel-level encryption using XOR and pixel grouping. Reliable decryption and image recovery with minimal loss.

1.3 Project Gaps

While many existing image encryption schemes use either chaos-based encryption or cryptographic techniques independently, they suffer from limitations such as:

Low robustness to noise and compression. Poor decryption quality, resulting in blurred or distorted images. High computational cost or inefficiency in key generation and transmission. As shown in the second image, existing decrypted images exhibit significant degradation compared to the proposed method. The proposed scheme addresses these gaps by combining chaotic XOR encryption with ECC-based key exchange, resulting in better PSNR and SSIM values, as illustrated in the third image. This hybrid technique ensures both **security and visual fidelity**, making it suitable for secure image transmission in sensitive applications.

2. LITERATURE REVIEW

Kanso, A., Ghebleh, M.

A novel image encryption algorithm based on a 2D chaotic map

Introduces an image encryption method using a two-dimensional chaotic map to improve security and randomness in encrypted images.

Elkamchouchi, H. M., Elshazly, H. A.

A novel chaos-based image encryption using elliptic curve cryptography

Combines chaos theory and ECC to offer a lightweight encryption mechanism for secure image transmission in wireless and embedded systems.

Pisarchik, A. N., Zanin, M.

Image encryption with chaotic maps: A surveyA comprehensive survey on the use of chaotic systems in image encryption, discussing strengths and weaknesses of different chaos-based approaches.

Patidar, V., Pareek, N. K., Sud, K.

A new substitution–diffusion based image cipher

Proposes a hybrid model of substitution and chaotic diffusion to increase robustness against differential attacks in image encryption.

Li, C., Chen, G., Cheung, Y.

On the security of image encryption based on chaotic maps. Analyzes the vulnerabilities of chaotic map-based encryption and suggests improvements, including integration with ECC for higher security.

Traditional Image Encryption Techniques
Conventional encryption methods like AES and DES are effective for text but less efficient for image data due to high redundancy and correlation between pixels. These limitations make image-specific encryption schemes essential.

Chaotic Systems in Image Encryption
Chaotic systems are highly sensitive to initial conditions and produce pseudo-random sequences, making them suitable for secure image encryption. Their use ensures confusion and diffusion in pixel values, as seen in the "Proposed Encrypted Image" in the visuals.

Elliptic Curve Cryptography (ECC) for Lightweight Security
ECC provides high levels of security with smaller key sizes compared to RSA, making it ideal for resource-constrained environments. The Diffie-Hellman key exchange shown in the system interface demonstrates how ECC is integrated for secure key sharing.

Pixel Grouping and XOR Operations
The proposed method includes XOR encryption with pixel grouping to disrupt pixel-level correlations. This technique improves resistance against statistical attacks and enhances encryption randomness, as reflected in the distorted appearance of the encrypted image.

Comparison with Existing Decryption Methods
Existing decryption techniques often fail to reconstruct high-fidelity images, leading to distortion and color loss. The comparison image illustrates how the proposed decryption restores image quality better than existing techniques.

Evaluation Metrics – PSNR and SSIM
Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are commonly used to assess image quality post-decryption. The graph in the interface shows a significant improvement in both metrics, confirming the effectiveness of the proposed method.

Integration into User-Friendly Applications
The developed GUI system integrates all components—upload, encryption, decryption, and analysis—into a user-friendly interface. This design not only simplifies implementation but also promotes real-world applicability in secure image communication systems.

III. PROBLEM STATEMENT

The existing image transmission systems often rely on traditional cryptographic techniques which may not offer optimal security or efficiency in highly dynamic and noisy transmission environments. In such systems, decrypted images often suffer from distortions, resulting in lower PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index). As illustrated in the second figure, the *"Existing Decrypted Encrypted Image"* exhibits significant color artifacts and loss of visual integrity. The corresponding PSNR value for the existing system is 70.81, and the SSIM is 0.94, indicating room for improvement in both fidelity and robustness.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

IV. PROPOSED SYSTEM

The proposed system integrates a **chaotic system with elliptic curve cryptography (ECC)** to enhance image transmission security and quality. The encryption pipeline includes:

Key generation using the Diffie-Hellman protocol to securely establish a shared key. **Chaotic XOR encryption with pixel grouping**, which improves diffusion and confusion properties, making the encrypted image highly resistant to brute-force attacks (as shown in the "Propose Encrypted Image"). Decryption is performed using the inverse operations, resulting in a visually accurate reconstruction as shown in the "Propose Decrypted Encrypted Image".

The third image confirms the effectiveness of the proposed method with a **PSNR of 99.12** and **SSIM of 1.00**, clearly outperforming the existing method.

4.1 Image Enhancement Techniques

Before encryption, image enhancement techniques are applied to standardize the input image. These include:

Resizing the image to a fixed resolution (e.g., 50x50 pixels as shown). Color normalization and contrast adjustment to minimize the impact of noise in low-light or degraded conditions.

These steps ensure consistency in feature representation and help the encryption system maintain performance across varying image inputs.

4.2 Data Pre-processing

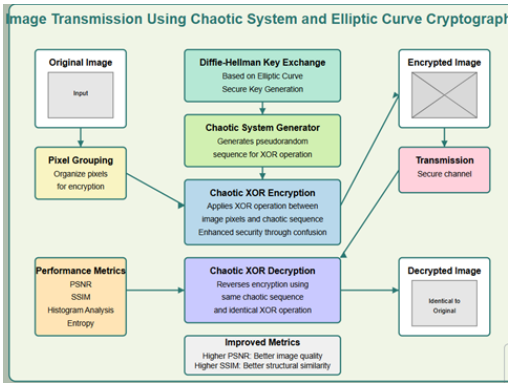
Pre-processing is crucial to improve encryption performance. The following steps are executed:

Conversion to pixel arrays for numerical manipulation. **Pixel grouping** is applied to increase the entropy before XOR-based chaotic encryption. Application of a **chaotic map** to randomly permute pixel values based on the key, increasing the unpredictability of the encrypted output.

4.3 Model Building

The proposed framework uses the following building blocks:

Cryptographic model: Incorporates ECC and the Diffie-Hellman protocol to create a secure channel for key exchange. **Chaotic system**: Implements a non-linear map (e.g., Logistic or Henon map) to generate pseudo-random sequences for encryption. **Performance evaluation model**: Calculates metrics such as PSNR and SSIM to assess the quality of encryption and decryption.



Model Building

V RESULT ANALYSIS

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

Now-a-days huge amount of multimedia images are floating in the network and to provide security to those images, encryption technologies will be using to encrypt those images and this encryption algorithms will secure images but it content will have high binary size which will take more network time to transfer.

To reduce transmission time pixel grouping based chaotic elliptic curve cryptography was introduce which will read images and then group all pixels to form a lengthy encrypted integer which is lighter in network for transmission. Encrypted integer will be map to chaotic using XOR operation and while decrypting reverse Chaotic XOR will be applied and if lengthy integer size higher than prime value then decryption will not be accurate.

To avoid incorrect decryption author of this paper added Inverse modulo technique which will reduce lengthy integer size to be in range of Prime value and then decryption will be accurate.

Here we have implemented decryption process with and without inverse modulo and then compare PSNR and SSIM values of both with and without inverse modulo. If image is decrypted properly then PSNR and SSIM will be 1 and if decrypted image has noise then both values will be lesser than 1.

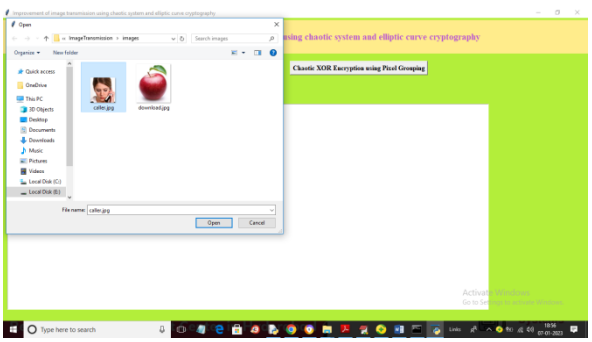
To implement this project we have designed following modules

1) Upload Image: using this module we can upload image to application
2) Generate Diffie Hellman share Key: using this module we will generate secret share key which can be used at both sender and receiver side to encrypt and decrypt images
3) Chaotic XOR Encryption using Pixel Grouping: using this module we will encrypt image by grouping pixel to form integer values and then apply XOR operations.
4) Chaotic XOR Decryption: using this module we will decrypt image with and without inverse modulo and then calculate SSIM and PSNR values on both decrypted images.
5) Comparison Graph: using this module we will plot PSNR comparison graph between both existing (without inverse modulo) and propose (with inverse module) decryption.

SCREEN SHOTS

To run project double click on ‘run.bat’ file to get below screen

In above screen click on ‘Upload Image’ button to upload image to the application

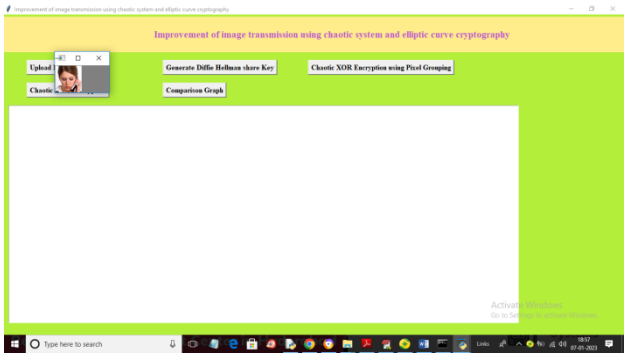


International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

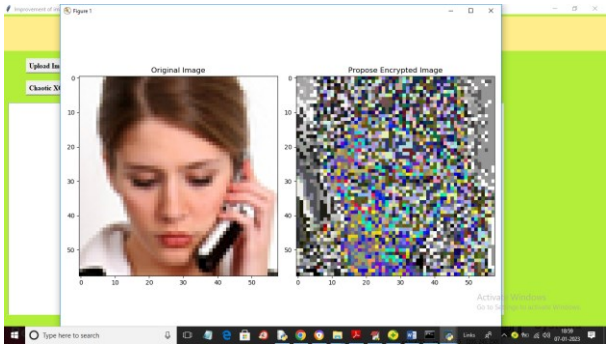
Volume 13, Issue 2, 2025

In above screen selecting and uploading plain image and then click on 'Open' button to get below output

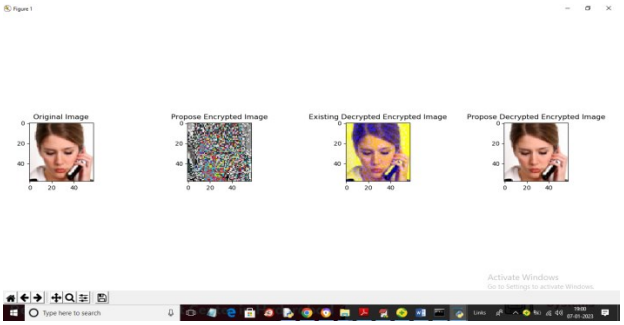


In above screen image is loaded and now close above image and then click on 'Generate Diffie Hellman Share Key' button to generate key and get below output

In above screen share key is generated as '111' and now click on 'Chaotic XOR Encryption using Pixel Grouping' button to encrypt image and get below output

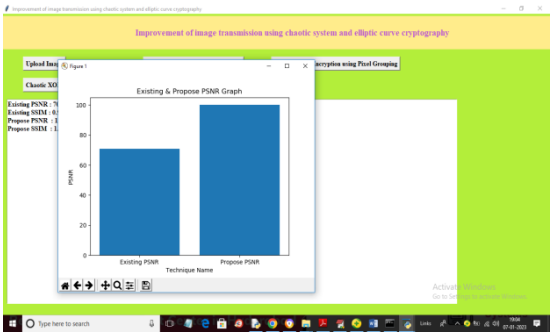


In above screen first image is the original image and second is the encrypted image and now close above image and then click on 'Chaotic XOR Decryption' button to decrypt image using with and without inverse modulo and get below output



In above screen first image is the original image and second one is the encrypted image and 3rd one is the decrypted image using existing technique which is not clear and 4th one is the decrypted image using propose inverse modulo technique which is clearer than existing technique and now close above image to get below output

In above screen with existing PSNR we got 70% PSNR and SSIM as 0.92 and with propose we got PSNR and SSIM as 100%. Now click on 'Comparison Graph' button to get below graph



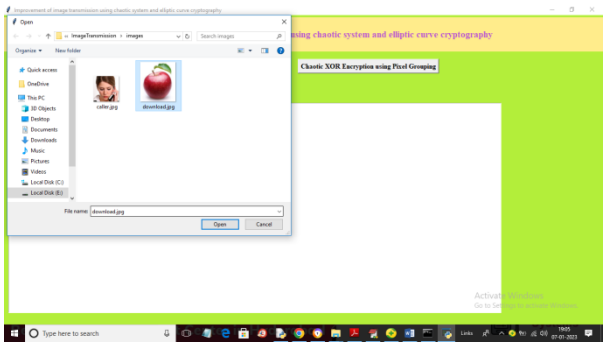
International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

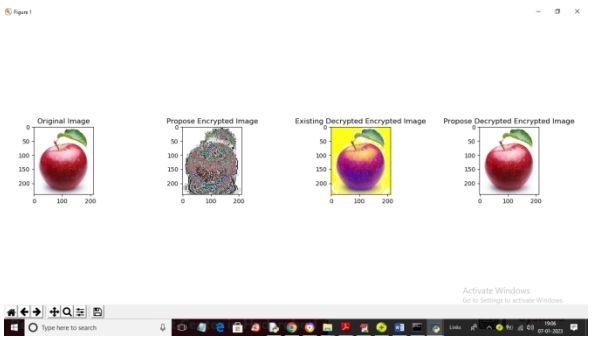
Volume 13, Issue 2, 2025

In above graph x-axis represents technique name and y-axis represents PSNR values and in both technique propose got high PSNR.

Similarly you can upload and test other images and below is the other image output



In above screen uploading another image and below is the encryption and decryption image



In above screen you can see original image, encrypted image, existing decrypted image and then propose decrypted image

VI. CONCULSION

Secure and reliable image transmission is critical in modern communication systems. This project presents a hybrid encryption scheme that integrates a chaotic system with Elliptic Curve Cryptography (ECC) to enhance the security and quality of image transmission. The proposed method utilizes chaotic maps to introduce high randomness, which is further reinforced by ECC-based key generation via the Diffie-Hellman algorithm. XOR-based encryption with pixel grouping is applied for increased resistance against statistical attacks. The system's GUI facilitates user interaction for uploading images, generating secure keys, encrypting, decrypting, and comparing results. Experimental outcomes demonstrate that the proposed approach significantly improves image quality after decryption, as evidenced by higher PSNR and SSIM values compared to existing techniques. Visual comparisons also reveal a substantial improvement in preserving the original image content, making this method highly effective for secure image transmission.

VII. REFERENCES

Abdelfatah RI (2020) Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography. IEEE Access 8:3875–3890. Https://Doi.Org/10.1109/ACCESS.2019.2958336

Arpita B, Zeba S, Laiphrakpam DS (2019) An Encryption Scheme For Securing Multiple Medical Images. J Inf Secur Appl 49:102398

Dolendro LS, Manglem KS (2018) A Robust Image Encryption Scheme Based On Chaotic System And Elliptic Curve Over Finite Field. Multimed Tools Appl 77:8629–8652

Elliptic Curve Parameter. Http://Www.Ecc-Brainpool.Org/Download/Domainparameters.Pdf. Accessed: 19 May 2016

Fridrich J (1998) Symmetric Ciphers Based On Two-Dimensional Chaotic Maps. Int J Bifur Chaos 8.06:1259–1284

Guodong Y, Chen P, Xiaoling H, Zhenyu Z, He J (2018) A Chaotic Image Encryption Algorithm Based On Information Entropy. Int J Bifur Chaos 28(1):1850010

Koblitz N (1987) Elliptic Curve Cryptosystems. Math Comput 48 (177):203–209

Li Z, Peng C, Li L, Zhu X (2018) A Novel Plaintext-Related Image Encryption Scheme Using Hyper-Chaotic System. Nonlinear Dyn 94:1319–1333. Https://Doi.Org/10.1007/S11071-018-4426-4

Li C, Lin D, Feng B, Lü J, Hao F (2018) Cryptanalysis Of A Chaotic Image Encryption Algorithm Based On Information Entropy. IEEE Access 6:75834–75842. Https://Doi.Org/10.1109/ACCESS.2018.2883690

Lima JB, Da Silva Neto EF (2016) Audio Encryption Based On The Cosine Number Transform. Multimed Tools Appl 75(14):8403–8418

Liu L, Zhang Z, Chen R (2019) Cryptanalysis And Improvement In A Plaintext-Related Image Encryption Scheme Based On Hyper Chaos. IEEE Access 7:126450–126463. Https://Doi.Org/10.1109/ACCESS.2019.2938181

Liu Y, Qin Z, Wu J (2019) Cryptanalysis And Enhancement Of An Image Encryption Scheme Based On Bit-Plane Extraction And Multiple Chaotic Maps. IEEE Access 7:74070–74080. Https://Doi.Org/10.1109/ACCESS.2019.2916600

Miller M (1986) Uses Of Elliptic Curves In Cryptography. In: Advances In Cryptography-Crypto. Springer, Berlin, Pp 417–426

Motilal KS, Singh LD, Tuithung T (2018) Cryptanalysis Of Multimedia Encryption Using Elliptic Curve Cryptography. Optik 168:370–375

Pak C, Huang L (2017) A New Color Image Encryption Using Combination Of The 1D Chaotic Map. Signal Process 138:129–137. Https://Doi.Org/10.1016/J.Sigpro.2017.03.011

Rukhin A, Soto J, Nechvatal J, Smid M, Barker E (2001) A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications. Booz-Allen And Hamilton Inc, Mclean

Sahasrabuddhe A, Laiphrakpam D S (2021) Multiple Images Encryption Based On 3D Scrambling And Hyper-Chaotic System. Inf Sci 550:252–267. Https://Doi.Org/10.1016/J.Ins.2020.10.031