www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1376-1380

e-ISSN : 2583-1062
Impact Factor : 7.001

ENHANCING SECURITY AND EFFICIENCY IN IMAGE ENCRYPTION WITH ECC AND HILL CIPHER TECHNIQUES

B. Sai Gopinadh[1], V. Venkata Jagan[2]

[1]Assistant Professor, Department Of BS&H, GMR Institute Of Technology, Rajam, Andhra Pradesh.

[2]B. Tech Student, Department Of Information Technology, GMR Institute Of Technology, Rajam, Andhra Pradesh.

ABSTRACT

In today's era of digital communication, the secure transmission of images is a significant concern due to vulnerabilities in existing encryption techniques. The Hill Cipher, a symmetric encryption algorithm, offers computational efficiency but is limited by the need to share private keys over unsecured channels, making it susceptible to attacks. Elliptic Curve Cryptography (ECC), on the other hand, is an asymmetric encryption technique known for its high security and computational efficiency. This paper introduces a novel hybrid image encryption technique that combines ECC and the Hill Cipher to enhance security and efficiency. The proposed system transforms the Hill Cipher into an asymmetric encryption method using ECC-generated keys, thus eliminating the need to exchange private keys. A self-invertible key matrix is used to streamline the decryption process, reducing computational overhead. The hybrid technique's performance is evaluated using metrics such as Entropy, Peak Signal-to-Noise Ratio (PSNR), and Unified Average Changing Intensity (UACI). Experimental results reveal that the proposed system achieves robust encryption with high security and computational efficiency, making it suitable for real-time multimedia and embedded system applications. the demand for effective image encryption techniques has surged, driven by the increasing reliance on the internet and various communication platforms for sharing sensitive visual content. The transmission of important images over unsecured channels poses significant risks, including potential attacks and unauthorized access. To mitigate these threats, encryption methods have emerged as essential tools for safeguarding images against malicious activities.

Keywords: Cryptographic security, Asymmetric encryption, Symmetric encryption, Elliptic Curve Discrete Logarithm Problem (ECDLP), Grayscale image encryption

1. INTRODUCTION

Among the various encryption techniques, the Hill cipher algorithm stands out as a symmetric encryption method characterized by its straightforward structure and rapid computation capabilities. However, its security is compromised due to the necessity for both the sender and receiver to share the same private key over potentially insecure channels. To address these vulnerabilities, this paper introduces a novel image encryption technique that integrates the Elliptic Curve Cryptosystem (ECC) with the Hill cipher, referred to as the ECCHC approach. This innovative method transforms the Hill cipher from a symmetric to an asymmetric encryption technique, thereby enhancing its With the increasing use of digital communication and multimedia applications, ensuring the security of image data has become crucial. Images transmitted over public channels are vulnerable to interception and unauthorized access, necessitating robust encryption mechanisms. Cryptographic methods can be broadly categorized into symmetric and asymmetric techniques. Symmetric algorithms, such as the Hill Cipher, utilize the same key for encryption and decryption, offering simplicity and speed. However, their reliance on shared private keys over insecure channels makes them susceptible to various attacks. Asymmetric cryptographic techniques, such as Elliptic Curve Cryptography (ECC), use separate public and private keys, enhancing security by eliminating the need for key sharing. ECC is particularly advantageous due to its high security and efficiency, even with smaller key sizes. Combining ECC with the Hill Cipher can leverage the strengths of both techniques, resulting in a robust hybrid encryption approach.

The proposed approach utilizes a self-invertible key matrix to generate both encryption and decryption keys, eliminating the need for the decryption process to compute the inverse of the key matrix. For demonstration purposes, a 4x4 secret key matrix is employed in this study. The effectiveness of the grayscale image encryption is evaluated using several metrics, including Entropy, Peak Signal to Noise Ratio (PSNR), and Unified Average Changing Intensity (UACI). These measures facilitate a comprehensive comparison between the encrypted images and their original counterparts, allowing for an assessment of the performance of the proposed encryption technique.

This paper proposes a hybrid encryption method, termed Elliptic Curve Cryptography and Hill Cipher (ECCHC), which transforms the symmetric Hill Cipher into an asymmetric technique. ECC is used to generate private and public keys, and a self-invertible key matrix simplifies the decryption process. The system's efficiency is assessed using grayscale images and evaluated based on Entropy, PSNR, and UACI metrics.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1376-1380
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

2. LITERATURE REVIEW

In recent years, the demand for robust image encryption techniques has led to numerous advancements in cryptographic systems. Symmetric encryption techniques, such as the Hill Cipher, have been widely studied for their computational simplicity and speed. However, they face critical challenges, including key distribution vulnerabilities. Researchers have proposed several modifications to enhance the security of the Hill Cipher. For example, Ismail et al. (2006) introduced a variant that uses a different key for each plaintext block, improving security against certain attacks. Similarly, Acharya et al. (2009) proposed an advanced Hill Cipher algorithm that employs a self-invertible matrix, eliminating the need for matrix inversion during decryption.

On the other hand, asymmetric encryption techniques, particularly those based on Elliptic Curve Cryptography (ECC), have gained significant attention for their high security and efficiency. ECC was first proposed by Miller (1985) and Koblitz (1987), and its security relies on the computational difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). ECC has been extensively used in various applications, including secure communication and digital signatures, due to its smaller key sizes and lower computational overhead compared to other public-key systems like RSA.

Hybrid cryptographic approaches combining symmetric and asymmetric techniques have been explored to leverage the advantages of both methods. Agrawal and Gera (2014) proposed a system that integrates ECC with the Hill Cipher, where ECC is used to secure key distribution, and the Hill Cipher is used for data encryption. While effective, this approach increases computational complexity due to additional operations like scalar multiplication in ECC.

Several metrics have been used to evaluate the effectiveness of encryption techniques. Entropy, a statistical measure of randomness, is commonly used to assess the security of encrypted images. Higher entropy values indicate stronger encryption. Metrics such as Peak Signal-to-Noise Ratio (PSNR) and Unified Average Changing Intensity (UACI) evaluate the quality of encryption and its resistance to differential attacks.

Building on these advancements, this study combines ECC with a self-invertible Hill Cipher to create a robust hybrid encryption system. By leveraging ECC for key generation and distribution, the proposed method addresses the key-sharing vulnerabilities of the Hill Cipher. The use of a self-invertible key matrix further simplifies the decryption process, making the system computationally efficient while maintaining high security.

Elliptic Curve Cryptography (ECC)

ECC is a public-key cryptographic technique based on the mathematics of elliptic curves. It offers high security with minimal computational overhead, making it ideal for resource-constrained environments.

Definition: An elliptic curve over a finite field is defined by the equation: The condition ensures the curve has no singularities.

Operations

Key operations in ECC include:

1. **Point Addition:** Combines two points and on the curve to produce a third point .
2. **Point Doubling:** Adds a point to itself to generate a new point .
3. **Scalar Multiplication:** Computes , where is an integer, by repeated point addition. This operation forms the basis of ECC encryption and decryption.

ECC's security relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), making it resistant to brute-force and other common cryptographic attacks.

Hill Cipher Algorithm

The Hill Cipher is a symmetric block cipher introduced by Lester Hill in 1929. It encrypts plaintext by dividing it into fixed-size blocks and performing matrix multiplication with a key matrix.

Encryption

Given a key matrix of size and a plaintext vector of size , the ciphertext is calculated as:

Decryption

Decryption requires the inverse of the key matrix (K^{-1}":

One limitation of the Hill Cipher is that the inverse key matrix may not always exist, making decryption impossible in some cases. Additionally, the reliance on shared keys over unsecured channels compromises its security.

3. METHODOLOGY

Proposed Hybrid Cryptosystem

The proposed ECCHC method integrates ECC with the Hill Cipher to address the latter's limitations. ECC is used to generate private and public keys, eliminating the need for key sharing. A self-invertible key matrix ensures efficient decryption without computing matrix inverses.

Key Generation

1. **Elliptic Curve Parameters:** Both sender and receiver agree on an elliptic curve and its parameters is the generator point.
2. **Private and Public Keys:** The sender and receiver choose private keys and and compute public keys (P_A = n_A \cdot G" and (P_B = n_B \cdot G").
3. **Shared Key:** A shared key is derived.
4. **Self-Invertible Key Matrix:** A 4x4 self-invertible matrix is constructed using the shared key components, ensuring efficient encryption and decryption.

Encryption Process

1. Divide the image into 4-pixel blocks and represent each block as a vector .
2. Multiply each vector by the self-invertible key matrix :
3. Reconstruct the encrypted image from the resulting vectors.

Decryption Process

1. Divide the encrypted image into 4-pixel blocks and represent each block as a vector .
2. Multiply each vector by the self-invertible key matrix :
3. Reconstruct the decrypted image from the resulting vectors.
4. Performance Evaluation
5. The ECCHC system's performance is evaluated using the following metrics:
6. Entropy
7. Entropy measures the randomness in an encrypted image. Higher entropy values indicate stronger encryption. For grayscale images, the ideal entropy value is 8.
8. Peak Signal-to-Noise Ratio (PSNR)
9. PSNR assesses the quality of the decrypted image by comparing it to the original. Higher PSNR values indicate minimal distortion, which is critical for effective encryption.
10. Unified Average Changing Intensity (UACI)
11. UACI measures the average intensity change between the original and encrypted images. Higher UACI values indicate resistance to differential attacks.

4. EXPERIMENTAL RESULTS

The ECCHC Method was tested on grayscale images of size 256x256 pixels. Results show:

1. **Entropy:** The proposed method achieved values close to the ideal (e.g., 7.997 for the Lena image), surpassing existing techniques.
2. **PSNR:** Values such as 8.58 dB reflect negligible data loss in decryption.
3. **UACI:** Values near the expected 33.46% indicate strong resistance to attacks.
4. **Computation Time:** The encryption and decryption processes required approximately 1.26 seconds per image, demonstrating the system's efficiency.

5. CONCLUSION

The proposed ECCHC method combines the security of ECC with the computational efficiency of the Hill Cipher, addressing the limitations of traditional symmetric encryption. By employing a self-invertible key matrix, the system eliminates the need for matrix inversion during decryption, reducing computational overhead. Experimental results confirm that ECCHC provides robust encryption with high security and efficiency, making it suitable for real-time multimedia and embedded system applications. Future work will extend the method to support RGB images and multimedia data. The evaluation of the ECCHC technique through metrics such as Entropy, Peak Signal to Noise Ratio (PSNR), and Unified Average Changing Intensity (UACI) demonstrates its effectiveness in preserving image quality

while ensuring robust encryption. The results indicate that the proposed method achieves high levels of randomness and security, making it resistant to various forms of cryptographic attacks.

As the demand for secure image transmission continues to grow in various applications, including healthcare, finance, and personal communication, the ECCHC technique offers a viable solution that balances security and computational efficiency. Future work may explore the adaptation of this approach for RGB images and real-time multimedia applications, further expanding its applicability in diverse contexts.

6. REFERENCES

[1] Acharya, B., Rath, G. S., Patra, S. K., & Panigrahy, S. K. (2009). Image encryption using advanced Hill cipher algorithm. International Journal of Recent Trends in Engineering, 1(1), 25-29.

[2] Agrawal, K., & Gera, A. (2014). Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Cryptosystem. International Journal of Computer Applications, 106(1), 18-22.

[3] Ismail, I. A., Amin, M., & Diab, H. (2006). How to repair the Hill cipher. Journal of Zhejiang University-SCIENCE A, 7(12), 2022-2030.

[4] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203-209.

[5] Miller, V. S. (1985). Use of elliptic curves in cryptography. Advances in Cryptology—CRYPTO 85 Proceedings, 417-426.

[6] Panduranga, H. T., & Naveen Kumar, S. K. (2012). Advanced partial image encryption using two-stage Hill cipher technique. International Journal of Computer Applications, 60(16), 21-25.

[7] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

[8] Gutub, A. A. A., & Khan, E. A. (2012). Hybrid crypto hardware utilizing symmetric-key and public-key cryptosystems. Advanced Computer Science Applications and Technologies (ACSAT), IEEE, 116-121.

[9] Rahman, M. N. A., Abidin, A. F. A., Yusof, M. K., & Usop, N. S. M. (2013). Cryptography: A new approach of classical Hill cipher. International Journal of Security and Its Applications, 7(2), 179-190.

[10] Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 31-38.

[11] Sharma, N., & Chirgaiya, S. (2014). A novel approach to Hill cipher. International Journal of Computer Applications, 108(11), 5-9.

[12] Mahmoud, A., & Chefranov, A. (2014). Hill cipher modification based on pseudo-random eigenvalues. Applied Mathematics, 8(2), 505-516.

[13] Rajput, Y., & Gulve, A. K. (2014). A comparative performance analysis of an image encryption technique using extended Hill cipher. International Journal of Computer Applications, 95(4), 16-20.

[14] Gutub, A. A. A., & Ibrahim, M. K. (2003). Power-time flexible architecture for GF(2k) elliptic curve cryptosystem computation. Proceedings of the 13th ACM Great Lakes Symposium on VLSI, 237-240.

[15] Hamissa, G., Sarhan, A., Abdelkader, H., & Fahmy, M. (2011). Securing JPEG architecture based on enhanced chaotic Hill cipher algorithm. Computer Engineering & Systems (ICCES), 2011 International Conference on, IEEE, 260-266.

[16] Naskar, P. K., & Chaudhuri, A. (2014). A secure symmetric image encryption based on bit-wise operation. International Journal of Image, Graphics & Signal Processing, 6(2), 30-38.

[17] Bokhari, M. U., & Shallal, Q. M. (2016). A review on symmetric key encryption techniques in cryptography. International Journal of Computer Applications, 147(10), 14-19.

[18] Naveen Kumar, S. K., Sharath Kumar, S. K., & Panduranga, H. T. (2012). Encryption approach for images using bits rotation reversal and extended Hill cipher techniques. International Journal of Computer Applications, 59(16), 5-11.

[19] Nandi, S., & Karforma, S. (2017). A comparative study of various image encryption techniques. International Journal of Computer Applications, 169(7), 8-15.

[20] Wu, X., & Noonan, J. P. (2013). Efficient image encryption techniques: A survey. Image and Vision Computing, 31(6), 459-475.

[21] Darrel, H., Menezes, A., & Vanstone, S. (2004). Guide to elliptic curve cryptography. Springer-Verlag Professional Computing Series.

[22] Alese, B. K., Philemon, E. D., & Falaki, S. O. (2012). Comparative analysis of public-key encryption schemes. International Journal of Engineering and Technology, 2(9), 1552-1568.

[23] Gutub, A. A. A., Tabakh, A. A., Al-Qahtani, A., & Amin, A. (2013). Serial vs. parallel elliptic curve crypto processor designs. IADIS International Conference Applied Computing.

[24] Nayak, B. (2014). Signcryption schemes based on elliptic curve cryptography (Master's Thesis). National Institute of Technology Rourkela, India.

[25] Panduranga, H. T., & Naveen Kumar, S. K. (2012). Hybrid approach for dual image encryption using nibble exchange and Hill-cipher. Machine Vision and Image Processing (MVIP), IEEE International Conference, 101-104.