Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549833

IMAGE ENCRYPTION USING A COMBINATION OF THE HILL CIPHER, FIBONACCI MATRIX, AND ELLIPTIC CURVE CRYPTOGRAPHY

S. Kaliswaran[1], M. Y. Mohamed Parvees[2]
[1]Research Scholar, Annamalai University, Chidambaram
[2]Research Supervisor, Annamalai University, Chidambaram
Email: kaliswaran1976@gmail.com

Abstract

Every day, the network transfers millions of photos. We want these photographs to be transferred securely because some of them are private and confidential. In order to communicate photos safely, cryptography is essential. To protect the data, in this paper The combination of Elliptic Curve, Hill Cipher and Fibonacci Matrix method is proposed. Elliptic Curve Cryptography (ECC) is an asymmetric key encryption and enhanced further using symmetric encryption of Hill Cipher allowing simple and fast computations over complex encryption methods of ECC. Hill cipher encryption algorithm is applied to each block using a randomly generated encryption key. Then Multiply each encrypted block by the Fibonacci matrix. This helps introduce additional complexity and adds a layer of security. The proposed image encryption algorithm tested using histogram analysis, entropy, and correlation coefficients.

Keywords: Elliptic Curve Cryptosystem, Fibonacci matrix, Hill Cipher, Image Encryption, Decryption.

1. INTRODUCTION:

The mathematical technique known as cryptography is used to protect text and image data from hackers and increase the security of communication mediums. Before sending an image over the internet to the recipient, the sender performs encryption, turning the original plain image into an encrypted image. Decryption is carried out at the receiver's end, converting the encrypted (ciphered) image back to its original state. The security of content in photos on the web has become a hot concern as usage of images has skyrocketed. Consequently, the researchers developed a number of image encryption techniques. These algorithms employ both symmetric (private-key) and asymmetric (public-key) encryption techniques (Simmons, 1979). The same key is used for both encryption and decryption in symmetric encryption. These algorithms work well and quickly, especially when dealing with big amounts of data like photos (Huang et al., 2019; Luo et al., 2018; Setyaningsih et al., 2020). The management and distribution of keys, however, is a significant flaw with symmetric encryption. The key must be securely transmitted over the network, but attackers may be able to intercept it in transit. In fact, the number of keys will suddenly expand as the number of users does, burdening the network.

These problems are solved by the asymmetric (public key encryption, or PKE), which uses two keys (public and private) that are utilised independently for encryption and decryption. It is challenging to extract the private key from the public key. Therefore, since the receiver has his own private key, there is no need to exchange the private key under this encryption. As a result, the key distribution problem does not affect encryption. Additionally,

it can offer a digital signature capability that is not possible with symmetric encryption. Digital signatures provide non-repudiation, message integrity, and authentication services. The discrete logarithmic issue and the factorization problem are the two most challenging mathematical problems in public key encryption. Digital signature algorithm (DSA) and Rivest-Shamir-Adleman both exploit these two types of issues.

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. It has poor as the sender and receiver share the same private key while transmitting the data over unsecured channel. Several researchers made an effort to develop and enhance the security of hill cipher technique. In (Ismail et al., 2006) the author designed an approach called Hill Multiplying Rows by Initial Vector (HillMRIV) algorithm. This algorithm generates different keys for encrypting each block of plaintext rather than using single matrix key for all plaintext blocks. This improves hill cipher algorithm security, but fails when the plaintext blocks contain only zeros. A new approach Advanced hill algorithm (AdvHill) (Acharya et al., 2007) is designed, to solve the problem of decryption when the key matrix inverse doesn't exist. AdvHill algorithm generates an involutory key matrix, and the encryption and decryption are performed with the same key matrix. So, it decreases the computations because there is no need to obtain the inverse key matrix by the recipient and the improved cipher randomization increases the algorithm performance compared to the initial Hill cipher. In (Khazaei & Ahmadi 2017) the author strengthens the divide-and conquer ciphertext only attack on hill cipher using Chinese Remainder Theorem on the code complexity of O(d13d) with a slightly higher data complexity cost. Evaluating the results of the proposed system or justifying their optimality on the basis of reasonable assumptions about computational complexity is still an open issue. In (M Essaid et al., 2012) designed an algorithm to make the encryption technique more efficient, by encrypting all kinds of images pixel by pixel, even with the images having black background or the adjacent pixels of image having high correlation.

The remaining of this paper arranged as: Section 2 briefly explains the preliminaries of the elliptic curve cryptography, its operation and hill cipher. The proposed method is discussed in section 3. The experimental results of the proposed method are presented in section 4. In Section 4 security analysis of the proposed method explained. Finally, the conclusion is presented in the section 5.

2. BACKGROUND

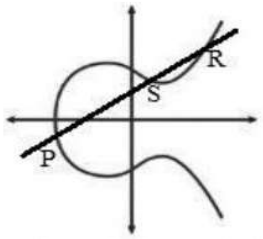
In this section, the elliptic curve cryptography, its operations and hill cipher are discussed

2.1 Elliptic curve cryptography

ECC is a public-key encryption algorithm based on the elliptic curve defined over a finite field. ECC is a modern encryption algorithm that provides greater security with shorter key lengths, allowing it to be used by devices with less computational power like smartphones to communicate securely over the internet.

The representation of Elliptic curve is $Ep\ (a, b)$ where a, b are confined to $mod\ p$ and p is a prime number. The Weierstrass normal form, the fundamental Elliptic curve E utilized for cryptography is in the form E: $y2 = (x3 + ax + b)\ mod\ p$ over a prime field Fp which is represented in Fig. 1. Here a, $b \in Fp$, $p \neq 2$, 3 and the curve should satisfy the condition $4a3 + 27b2 \neq 0$ called Non-Singular Elliptic Curve, then it has 3 distinct roots which is suitable

for ECC. The elliptic curve group $Ep\ (a, b)$ includes all (x, y) points which satisfies the elliptic curve E along with an additional point O called as point to infinity.



$y^2 = x^3 + ax + b$

Figure 1 Points on Elliptic curve

2.1 Operations:

2.1.1 Point addition:

Suppose P1 = (x1, y1) and P2 = (x2, y2), where P1 ≠ P2, are two points lie on an elliptic curve E. Adding the two points P1 and P2 giving a third point R that should lie on the same curve E.

$$s = \frac{(y2 - y1)}{(x2 - x1)} \quad R = P_1 + P_2 = (x_3, y_3) \text{ where } x_3 = s^2 - x_1 - x_2 \,, y_3 = s(x_1 - x^2) - y1$$

2.1.2 Point doubling:

Adding the point P1 = (x1, y1) that lies on the elliptic curve E to itself is called point doubling. The point R that results from doubling the point P is also lies on the elliptic curve E.

$$R = 2P = P + P = (x_3, y_3) \text{ where } s = 3x_1^2 + a / 2y_1$$

$$x_3 = (s^2 - 2x_1) \pmod p \,, y_3 = (sx_1 - sx_3 - y1) \pmod p$$

2.1.3 Scalar Multiplication:

Scalar multiplication is the main operation on EC that consumes more time in encryption and decryption operations, it depends on point addition and point doubling.

$$R = kP = P + P + P + \cdots + P \text{ (k times)}$$

An effective algorithm to solve point multiplication can be shown as an example:

$$R = 15P = 2(2(2P + P) + P) + P$$

The scalar multiplication of an integer k by the point P = (x1, y1) that lies on the curve E can be defined by repeating the addition of the point P to itself k times. The result point R also lies on the elliptic curve E.

2.2 Hill Cipher

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. To encrypt a image, each block of n pixel (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 256. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

2.3 Fibonacci Q-matrix

The elements of the Fibonacci sequence, F_n,

$$F_n = F_{n-1} + F_{n-2}\ ,\ n > 1$$

where $F_1 = F_2 = 1$.

The Fibonacci Q matrix is given by:

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

The nth power of the Fibonacci Q matrix is the matrix defined by:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$$

where F_n is the Fibonacci number, and the determinants of the Fibonacci Q-matrix is:

$$Det(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

The inverse matrix Q^{-n} has the following form:

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix}$$

3. PROPOSED METHOD

In this section the proposed encryption and decryption algorithm is discussed in detail. The proposed algorithm uses ECC, Hill cipher and Fibonacci matrix. The encryption and decryption of the image using this algorithm is described as follows:

Assume that two users are in communication, the User A (sender) transmit the information in the form of an image (PI) to the User B (receiver) through an insecure medium. Initially the elliptic curve E should be agreed by both the Users, and the domain parameters over Fp are shared $\{p, a, b, G, n, h\}$, where p is large prime integer, $a, b \in FP$ are the coefficients specifying an elliptic curve E, G is the base point on E, n is a random integer specifying FP, h is the cofactor. Later, from the interval [1,2,3 …, $p-1$] each user has to select their private key randomly; nA for User A (sender) and nB for User B (receiver).

The public key generation of User A and User B are as follows:

PA = nA. G

PB = nB. G

In order to obtain the initial key KI, every user performs multiplication on their private key with the other user's public key.

KI= nA. PB = (x, y) then

Compute K1 = x.G = (k11, k12) and K2 = y. G = (k21, k22)

By performing this Elliptic curve key generation, both the users generate the keys K1 and K2 and it is written in the form of 4 × 4 key matrix Km.

$$Km = \binom{k1}{k2}$$

Now, we find Fibonacci Q matrix as:

$$\text{Fm} = \text{km} * \begin{bmatrix} Fn+1 & Fn \\ Fn & Fn-1 \end{bmatrix}$$

Encryption Process:

1. Generate an ECC key pair:
   - Generate a private key and corresponding public key using ECC algorithms.
   - Keep the private key secure, and share the public key with the intended recipient.
2. Convert the image into a matrix:
   - Represent the image as a matrix, where each element represents a pixel value.
   - Apply any necessary preprocessing, such as converting the image to grayscale or resizing.
3. Apply the Hill cipher:
   - Divide the image matrix into smaller blocks, depending on the chosen block size for the Hill cipher.
   - Apply the Hill cipher encryption algorithm to each block using a randomly generated encryption key.
4. Apply the Fibonacci matrix transformation:
   - Multiply each encrypted block by the Fibonacci matrix element-wise.
   - This step helps introduce additional complexity and adds a layer of security.
5. Encrypt the Hill cipher key using ECC:
   - Encrypt the randomly generated Hill cipher key using the recipient's public key obtained from ECC.
   - This step ensures that even if the encrypted image and Fibonacci matrix are intercepted, they cannot be decrypted without the corresponding private key.
6. Combine the encrypted blocks and the encrypted Hill cipher key:
   - Concatenate the encrypted blocks and the encrypted Hill cipher key into a single data structure or file.
   - Transmit this combined data securely to the recipient.

Decryption Process:

1. Decrypt the Hill cipher key using the recipient's private key obtained from ECC.
2. Use the decrypted Hill cipher key to reverse the Fibonacci matrix transformation on the encrypted blocks.
3. Apply the inverse Hill cipher algorithm to each block to obtain the original image matrix.
4. Convert the matrix back into an image representation.
5. Display or save the decrypted image.

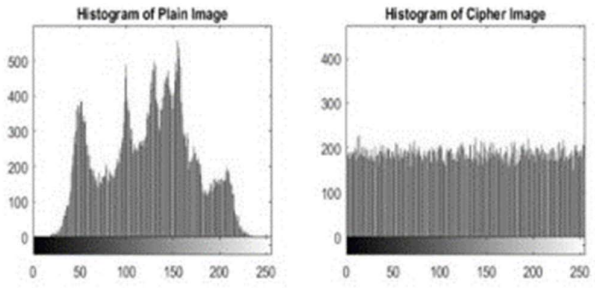
Proposed Encryption Algorithm:

4. EXPERIMENTAL ANALYSIS RESULTS:

4.1 Histogram Analysis

The Intensity Variation is a very helpful way to evaluate the effects on the picture of encryption and the distribution of the pixel's intensity in that image. If the histogram is more uniform then it represents a good diffusion and hence the encryption is stronger which can resist the statistical attacks. In the Figure. 1 the original images Lena and its corresponding original and cipher image histograms are displayed. It is noticed that the original and cipher images histograms are completely different and the cipher images histogram distributions are uniform. Clearly, from the encrypted image there is no useful information can be taken hence, ensuring high security. It indicates that the algorithm suggested has better capacity of opposing statistical attacks successfully.

Fig 1. Original Image of Lena



4.2 Entropy Analysis

The concept of information entropy solves the problem of quantifying and measuring information and can be used to judge the randomness of information. When the information entropy of a piece of information is close to its ideal value, we can judge that the information has good randomness. The information entropy of the image can be used to measure the degree of randomness of the image. The calculation method of information entropy is shown in formula, where represents the probability that each situation may occur in a model:

$$H(s) = -\sum_{i=1}^{n} p(i) \log_2 p(i),$$

Pixel values are distributed in the interval [0, 255], and the probability of each case is, so the information entropy of a grayscale image is 8 in an ideal case. If the information entropy of a grayscale image is close to 8, the image has good randomness. The information entropy of the cipher image of this algorithm is close to 8, and the result is not inferior to other algorithms. Therefore, it can be considered that the randomness of the cipher image of this algorithm meets the encryption requirements. The Table 1 displays the entropy values of the images executed in the proposed encryption algorithm.

Table 1 Information Entropy

Plain Image	Cipher Image
Lena	7.9986

4.3 Correlation Analysis

The correlation between adjacent pixels of the plaintext image is very strong. Breaking the correlation between adjacent pixels can enhance the ability of the encryption algorithm to resist statistical attacks. We randomly selected 10000 pixels from the original Lena image and the encrypted Lena image in the horizontal, vertical, and diagonal directions and listed these pixel values and their adjacent pixel values. There are strong correlations between adjacent pixels in the original Lena image, but there are almost no correlations between adjacent pixels in the encrypted Lena image. We can quantify the correlation between adjacent pixels with mathematical indicators. The correlation coefficient between adjacent pixels is calculated using formula, where is the mean, is the variance, and is the covariance. The correlation coefficients are shown in Table 2. By comparing the correlation coefficients of the original images and cipher images in Table 2.

$$\begin{cases} E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2, \\ \operatorname{cov}(x,y) = \dfrac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ r_{xy} = \dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \end{cases}$$

Table 2

Correlations of original images and encrypted images.

Images	Original image			Encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9688	0.9348	0.9010	0.0049	0.0002	0.0017

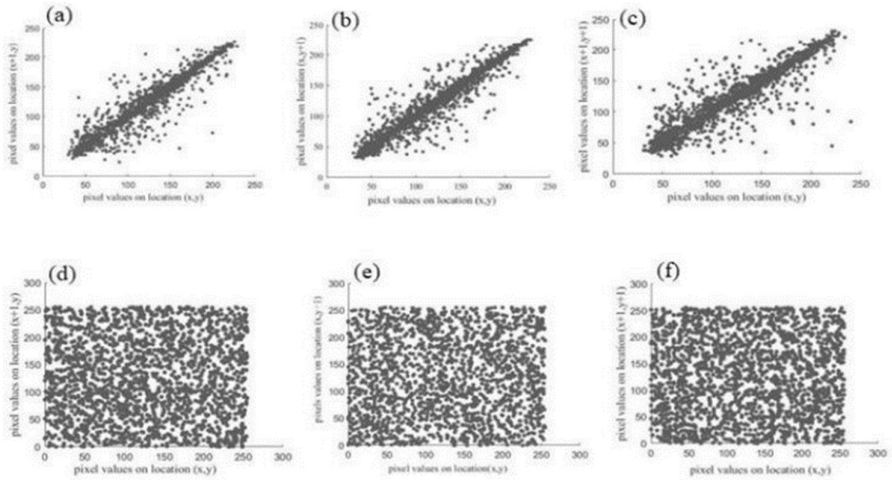


Fig 2. Adjacent pixel correlation of plain and cipher images of Lena. (a), (b), (c) Horizontal, vertical, diagonal directions in the plain image. (d), (e), (f) Horizontal, vertical, diagonal directions in the cipher image.

5. CONCLUSION

One of the most pressing challenges at the moment is data security. An efficient encryption technique is proposed in this paper. The combination of Elliptic Curve and Fibonacci Matrix and Hill Cipher method is proposed. Elliptic Curve Cryptography (ECC) is an asymmetric key encryption and enhanced further using symmetric encryption of Hill Cipher allowing simple and fast computations over complex encryption methods of ECC. hence, suitable for all applications and is reasonable for small gadgets to embedded systems. Currently, the proposed algorithm is applied on the grayscale images in this paper. Due to the advantages of the proposed encryption algorithm in future, it may be tested, used on RGB images and other modes of information such as audio and video to improve the transmission efficiency.

REFERENCES

1. Luo, Y., Zhou, R., Liu, J., Qiu, S., & Cao, Y. (2018). An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers. Multimedia Tools and Applications, 77(20), 26191-26217.
2. Song, J., & Lee, Y.H. (2021). Optical image encryption using different twiddle factors in the butterfly algorithm of fast Fourier transform. Optics Communications, 485, 126707.
3. Kaur, G., Agarwal, R., & Patidar, V. (2020). Chaos based multiple order optical transform for 2D image encryption. Engineering Science and Technology, an International Journal, 23(5), 998-1014.
4. Jiang, D., Liu, L., Zhu, L., Wang, X., Rong, X., & Chai, H. (2021). Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. Signal Processing, 188, 108220.
5. Wang, X., Feng, L., & Zhao, H. (2019). Fast image encryption algorithm based on parallel computing system. Information Sciences, 486, 340-358. Simmons, G.J. (1979). Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR), 11(4), 305-330.
6. Huang, L., Cai, S., Xiong, X., & Xiao, M. (2019). On symmetric color image encryption system with permutation-diffusion simultaneous operation. Optics and Lasers in Engineering, 115, 7-20.
7. Luo, Y., Tang, S., Qin, X., Cao, L., Jiang, F., & Liu, J. (2018). A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation. IEEE access, 6, 77740-77753.
8. Setyaningsih, E., Wardoyo, R., & Sari, A.K. (2020). Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution. Digital Communications and Networks, 6(4), 486-503.
9. Miller, V.S. (1986). Advances in Cryptology—CRYPTO'85 Proceedings. Use of elliptic curves in cryptography, 417-426.
10. Kobliz, N. (1987). Elliptic curve cryptography. Mathematics of Computation, 48, 203-209.
11. Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

12. Shankar, K., & Eswaran, P. (2016). An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In Artificial intelligence and evolutionary computations in engineering systems, 705-714.
13. Luo, Y., Ouyang, X., Liu, J., & Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access, 7, 38507-38522.
14. Khoirom, M.S., Laiphrakpam, D.S., & Themrichon, T. (2018). Cryptanalysis of multimedia encryption using elliptic curve cryptography. Optik, 168, 370-375.
15. Tawalbeh, L.A., Mowafi, M., & Aljoby, W. (2013). Use of elliptic curve cryptography for multimedia encryption. IET Information Security, 7(2), 67-74.
16. Hill, L.S. (1929). Cryptography in an algebraic alphabet. The American Mathematical Monthly, 36(6), 306-312.
17. Ismail, I.A., Amin, M., & Diab, H. (2006). How to repair the Hill cipher. Journal of Zhejiang University-Science A, 7(12), 2022-2030.
18. Acharya, B., Rath, G.S., Patra, S.K., & Panigrahy, S.K. (2007). Novel methods of generating self-invertible matrix for hill cipher algorithm.
19. Khazaei, S., & Ahmadi, S. (2017). Ciphertext-only attack on d× d Hill in O (d13d). Information Processing Letters, 118, 25-29.
20. Essaid, M., Akharraz, I., & Saaidi, A. (2019). Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps. Journal of Information Security and Applications, 47, 173-187.
21. Harwit, M. (2012). Hadamard transform optics. Elsevier. Qu, G., Meng, X., Yin, Y., Wu, H., Yang, X., Peng, X., & He, W. (2021). Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation. Optics and Lasers in Engineering, 137, 106392.
22. Zheng, P., & Huang, J. (2018). Efficient encrypted images filtering and transform coding with walsh-hadamard transform and parallelization. IEEE Transactions on Image Processing, 27(5), 2541-2556.
23. Prajwalasimha, S.N. (2019). Pseudo-Hadamard transformation-based image encryption scheme. In Integrated Intelligent Computing, Communication and Security, 575-583.
24. Devi, H.S., & Singh, K.M. (2020). Red-cyan anaglyph image watermarking using DWT, Hadamard transform and singular value decomposition for copyright protection. Journal of Information Security and Applications, 50, 102424.
25. Wang, X., Liang, X., Zheng, J., & Zhou, H. (2019). Fast detection and segmentation of partial image blur based on discrete Walsh–Hadamard transform. Signal Processing: Image Communication, 70, 47-56.
26. Anil K. Jain. (1989). Fundamentals of Digital Image Processing. Prentice Hall Inc., prentice hall international edition.