IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **Volume 11, Iss 11, Nov 2022**

EXPLORING SECURE IMAGE DISTRIBUTION WITH ELLIPTIC CURVE CRYPTOGRAPHIC METHODS

Shaik Mohammed Saleem,Student, Department Of C.S.E., K.S.R.M. College of Engineering (Autonomous), Kadapa, Y.S.R (D.t), Andhra Pradesh, India-516005.

S. Jaffer Hussain,Assistant Professor, Department Of C.S.E., K.S.R.M. College of Engineering (Autonomous), Kadapa, Y.S.R (D.t), Andhra Pradesh, India-516005.

Dr. V. Lokeswara Reddy, Professor &HoD, Department of CSE, K.S.R.M. College of Engineering (Autonomous), Kadapa, Y.S.R (D.t), Andhra Pradesh, India-516005.
Email id: vlreddy74@gmail.com

Abstract

In recent years, digital images have found extensive use across various applications. These applications can encompass social media platforms and crucial applications, such as those used in military and medical contexts. Nevertheless, cyber attacks and privacy issues pose significant security challenges for digital images. Consequently, various methodologies have been suggested to guarantee privacy and security. Cryptography is one of the first fields of study that comes to mind. Science has made great strides in the field of encryption. To keep sensitive information secret, encryption techniques are used. Multiple forms of encryption are used to keep digital photos private and unaltered. In-depth consideration is given to the Elliptic Curve Cryptography (ECC) image encryption method in this paper. This research examines how efficiently and securely images may be sent using ECC. ECC is a public key cryptography using elliptic curve mathematics to increase security. The study will likely look into how ECC can be used effectively in image sharing or distribution processes to ensure that photos are secure from unauthorized access and swiftly transferred. The experimental findings demonstrate that our approach yields superior outcomes concerning various evaluation indicators.

Keywords: **Digital images, privacy, security, cryptography, ECC, key distribution**.

1. Introduction

In the contemporary digital landscape, safeguarding digital media information is increasingly imperative. The proliferation of digital media can be attributed to the abundant online information. The method of visual cryptography involves the utilization of encryption technologies often employed in traditional cryptography to ensure the security of data. The watermarking technique is a widely employed approach for concealing data. In this context, due credit is attributed to Shamir for introducing a highly regarded mechanism for distributing confidential information, commonly called the cryptography method. Furthermore, Naor and Shamir have actively promoted the notion of visual cryptography as a means of image sharing [1].

The decryption process of an individual employing the comprehensive approach involving all 'n' shadows enables the retrieval of the image. However, the failure to possess even a solitary shade among the n shadows will result in significant difficulties for the individual in revealing any data included within the original image. Every individual shadow is imprinted into a separate transparency, and deciphering is accomplished through overlaying these shadows. The original image can only materialize when all "n" shadows are superimposed. Visual Cryptography or Visual Secret Sharing is a cryptographic technique employing a confidential sharing model for photographs. In this approach, decryption involves overlaying stacked shadows using the human visual mechanism [2].

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **© 2012 IJFANS. All Rights Reserved**, **Volume 11, Iss 11, Nov 2022**

Image security solutions aim to transform an image into an encrypted form that is highly resistant to comprehension and remains confidential among authorized users. This ensures that the image's content remains inaccessible to unauthorized individuals unless a decryption key is employed. The initial image magnitude can solely be obtained by identifying the key individual. Most standards regarding hardware and software employ the public key strategy for cryptographic procedures. ECC is a cryptographic system operating on public or asymmetric key cryptography principles. This implies that the encryption key and decryption keys employed in ECC are distinct from each other. Public key cryptography is a cryptographic system that utilizes a pair of keys, namely the private and public keys, to provide secure communication and data exchange. The distribution of public keys is extended to all users, while the private key utilized in the communication process remains exclusive to each user. In contrast to private key cryptography, ECC is well-suited for scenarios where a secure channel is unavailable for transmitting the private key. ECC is a recently developed cryptographic technique that offers enhanced security measures, reduced mathematical intricacy through lower key sizes, and improved computer efficiency.

The subsequent sections of this work are organised in the following manner. Section 2 provides a comprehensive explanation of the fundamental principles underlying digital photography and ECC. In the third section, the proposed technique is introduced and the workflow is outlined. The findings and relevant discussions are reported in Section 4. In conclusion, Section 5 provides a comprehensive summary and final remarks for the work.

2. Preliminaries

2.1 Digital Image Encryption

There are numerous options for encrypting digital images, including public-key and private-key systems like ECC, RSA, etc. In this work, we detail Encrypting images with an ECC key. The encryption process of a file is visually represented in Fig. 1. The procedure commences with the acquisition of photographs using a digital camera. Once a photo is taken, it is transformed into a matrix representation. This representation captures the intricate pixel values of the original image, ensuring that every nuance and detail is mapped within this matrix.

After acquiring the image's matrix, the next step is to encrypt it using ECC. ECC isfavored over more conventional cryptosystems because it can maintain the same level of security with comparatively shorter key lengths.Post encryption, if one attempts to view the image, it would be indecipherable, showcasing patterns and colors that would be nonsensical to the human eye. This indicates that the image's original content is securely hidden.However, the true prowess of any encryption method lies in scrambling the original information and its capability to revert the scrambled data to its original state. With the right decryption key and algorithm, the encrypted image undergoes decryption. At the culmination of this process, we obtain a plain, fully viewable image, which is faithfully represented in Fig. 2. This decrypted image retains all the details and attributes of the original photo, underscoring the efficacy and reliability of the encryption-decryption procedure using ECC.

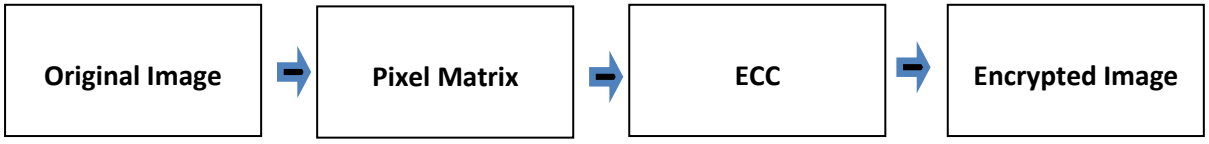

Fig.1. Digital Image Encryption

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **© 2012 IJFANS. All Rights Reserved**, Volume 11, Iss 11, Nov 2022

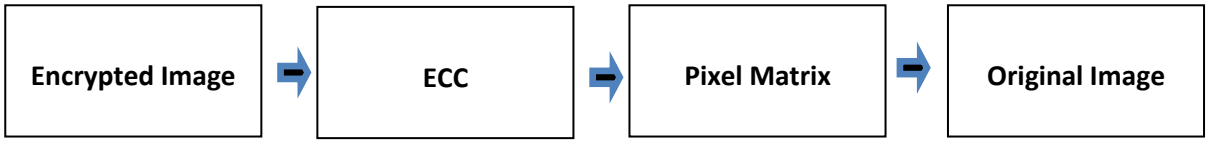

Fig.2. Digital Image Decryption

2.2 **ECC**

ECC is a contemporary cryptographic method widely recognized for its compactness, speed, and efficiency compared to existing alternatives. Bitcoin employs the ECC as its chosen asymmetric cryptosystem due to its notable efficiency and minimal computational requirements. The mathematical construct that facilitates these capabilities is the elliptic curve. Consequently, continue learning how these curves facilitate the most sophisticated cryptographic techniques globally.One prevalent application of ECC is the utilization of encryption techniques to safeguard data, ensuring that solely authorized entities possess the ability to decipher it. This technology possesses numerous evident applications, although its predominant usage pertains to Internet traffic encryption.

In the *boot.dev* web application uses ECC to encrypt a confirmation email, ensuring that only the intended recipient can comprehend the message's contents. A diverse range of public-key cryptography techniques exists, among which ECC is a singular variant. In this context, additional algorithms that can be considered are RSA, Diffie-Helman, and so on.To provide a foundational understanding for the subsequent discussion on ECC, reviewing the background of public-key cryptography is necessary. The authors strongly encourage you to research public-key cryptography more comprehensively whenever feasible [4].Public-key cryptography enables a range of functionalities to be achieved:

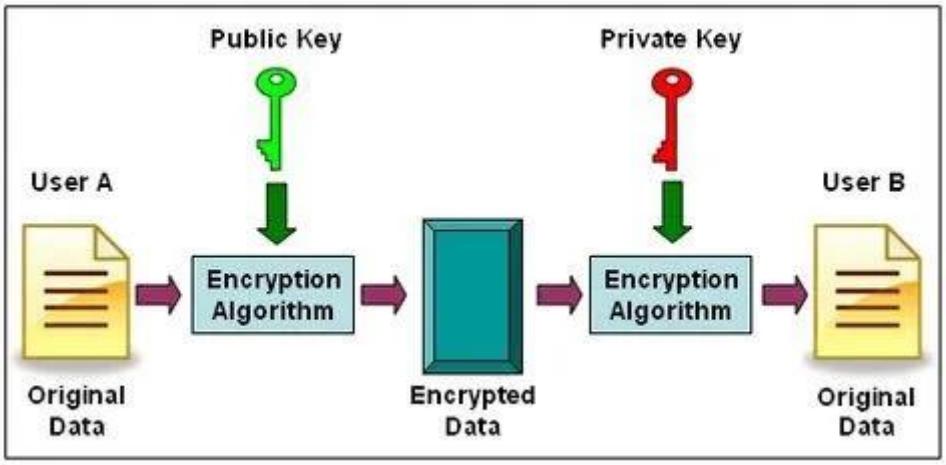

Fig. 3. Public-key cryptography

A pair of keys, known as a public key and a private key, are produced. Anyone can encrypt their own data now that the public key is freely available. However, the private key is guarded carefully, so that only authorised people can read the encrypted data. Figure 3 depicts the hypothetical situation.

2.3 Principle

The three parts of a code system are the plaintext, the key, and the ciphertext. The key might be considered public or private, or it can simultaneously be a hybrid of public and private. The author randomly chooses two points on the elliptic curve: A and B. These are the points A and B. On the elliptic curve, point B is designated the cardinal point, and A value is selected to satisfy the equation

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **© 2012 IJFANS. All Rights Reserved**, Volume 11, Iss 11, Nov 2022

A=kB. After that, designate the variable "A" as the public key and provide the value "k" to the variable that will serve as the private key. Obtaining the value of A is straightforward if you already know the value of k and B and want to use the additive group operation on an elliptic curve. However, if A and B are the only known variables, the problem of determining k becomes more difficult [5].

2.4 Advantages of ECC

ECC has a number of benefits. To begin, it's important to highlight the increased security demonstrated by ECC. When compared to other encryption algorithms, the ECC system is commonly considered to be the most effective at thwarting attacks. Its implementation offers enhanced security for websites and infrastructure, surpassing traditional encryption techniques. Consequently, ECC provides a more robust assurance for mobile Internet security [6].Additionally, it may be argued that ECC exhibits superior performance in the context of the mobile Internet. ECC employs a comparatively concise key length of 256 bits, occupying a smaller storage capacity. The increasing prevalence of mobile devices for conducting diverse online activities has prompted the adoption of ECC to enhance the consumer experience in mobile Internet security.Moreover, ECC exhibits superior features. ECC has the potential to offer enhanced security while utilizing reduced key lengths [7]. The comparative strength of 256-bit ECC is equivalent to that of a 3072-bit R.S.A. key. It is worth noting that the standard R.S.A.key length is currently set at 2048 bits. Based on the assessments conducted by reputable international entities, it has been determined that using the ECC algorithm on Apache and IIS servers results in a response time that exceeds R.S.A.'s by over 10 [8].

3. Related Works

This section comprehensively reviews digital picture encryption techniques utilizing ECC. As presented below, let us analyze the publications in which these studies were conducted.

Ye et al. [9] proposed using a double image as an encryption key. Two input photos are processed via discrete wavelet transformation to yield a quantization matrix with reduced data size. Using ECC, the matrices are encrypted. Images can be encrypted with the help of a revolutionary chaotic system implemented in an algorithm. Dawahdeh et al. [10] presented a method of encrypting images that draws on both the ECC and Hill cyphers. In contrast to its more common symmetric usage, the Hill cypher is used here as an asymmetric encryption method. The proposed encryption scheme makes use of a secret key represented as a 4x4 matrix with an inverse matrix. Therefore, the inverse matrix computation is superfluous during decryption.

Nagaraj et al. [11] presented a new method for encrypting images that makes use of ECC (ECC). A 4x4 magic matrix is used as the key in the suggested encryption method. Error Correction Codes are used to encrypt the resulting 8x8 data matrices from the picture conversion process. El-Latif et al. [12] published research that improved image encryption by combining a chaotic system with ECC. In this approach, a chaotic system is used to generate a new key stream. A pseudorandom bit sequence generated from points on a cyclic elliptic curve is then concatenated with this key stream. XOR algorithms are used to encrypt the image once it has been segmented into 8-bit data.

Singh et al. [13] introduced a technique for encrypting photos utilizing ECC. The image pixels are organized into groups based on the prime number of error correction codes to optimize the technique's efficiency under consideration. These groups are then transformed into large integers using the FromDigits algorithm. The IntegerDigits technique compresses all bits to a range of 0-255 to generate the encrypted image.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **© 2012 IJFANS. All Rights Reserved**, **Volume 11, Iss 11, Nov 2022**

In their study, Liu et al. [14] introduced an enhanced technique for picture encryption that utilizes chaotic maps and ECC as its foundation. The Menezes-Vanstone ECC algorithm generates the cryptographic keys. Encryption is achieved by combining a discrete chaotic map with a fractional two-dimensional triangle function.A method for encrypting images using ECC and Hilbert matrices was presented in a paper by Obaid et al. [15]. The technique employs a cryptographic secret key based on inverse matrices of 2x2 and 4x4 matrices. There will be no need to determine the inverse matrix during decryption. Bashir et al. [16] presented a new method of image encryption that combines ECC with a four-dimensional chaotic system. Each plain image is given a unique Hash-256 code to increase the method's security against plaintext/ciphertext assaults. These techniques allow the ECC to be distributed to its intended recipients by creating points for them without any waste.

The image encryption method using the Henon map, dynamic S-boxes, and ECC was described by Ibrahim et al. [17]. In this study, we show how the Henon map can be used to generate secure dynamic S-boxes. An image encryption method that is resistant to both chosen-plaintext and chosen-ciphertext assaults is developed using a dynamic S-box. Several different kinds of security algorithms work together to provide this protection. The ECC algorithm is used to generate the secret key, making it secure against any attacks.Azam et al. [18] presented an original method for encrypting photographs by using Mordell elliptic curves in their research. This research investigates how a public elliptic curve is chosen through a collaborative effort between a sender and a receiver.

The suggested method uses random numbers in conjunction with a dynamic S-box constructed on elliptic curves to mask and scramble pixels.In their research, Jasra and colleagues [19] presented several different methods that can be utilized to map images onto elliptic curves. In this work, a complete analysis of numerous major factors that determine the efficiency of a mapping technique has been provided. These characteristics include the fullness of the mapping, its reversibility, the bandwidth or quantity of bits utilized, the needed time, and the solution's cost-effectiveness.Some ways are utilized in this setting, such as binary grouping, pixel grouping, pixel intensity/points map tables, the Koblitz method, and generator point-based mapping. This research aims to do just that by examining the pluses and minuses of each of the listed methods.

Using chaotic systems and sophisticated ECC, the authors of [20] offer an encryption strategy. In addition, a pixel-grouping algorithm is incorporated to improve the encryption's overall efficiency. Nevertheless, this approach faces a limitation in the decryption process when the resulting number is either equal to or exceeds the elliptic curve's prime parameter (P). As mentioned, this study proposes a resolution to the difficultyof using the inverse modulo operator for integers higher than or equal to P. Additionally, it introduces a novel approach to circumvent comparable issues supported by empirical findings.

4. Proposed Method

The suggested technique facilitates the secure and confidential transmission of hidden images to the intended recipient. The visual representation is sent as shadows, consolidated to reconstruct the initial image. Using the pixel values, the suggested approach creates shadow representations. Extracted from the original image, the RGB image's pixel values are represented as a matrix with dimensions P*Q. The obtained pixel values are then used to build and reconstruct several shadows (labelled shadow1, shadow2, etc.). The reconstructed colour gradient is divided into several sections. The ECC method is used to encrypt the blocks that make up the colour bands. Next, the ECC decryption procedure is used to the encrypted image. The quality of the final product is then determined by contrasting it with the source image.Using objective measures like PSNR, MSE, CC of the system may be assessed. In Fig. 4 we see a block diagram of the hidden-photo-exchanging-protocol.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Iss 11, Nov 2022

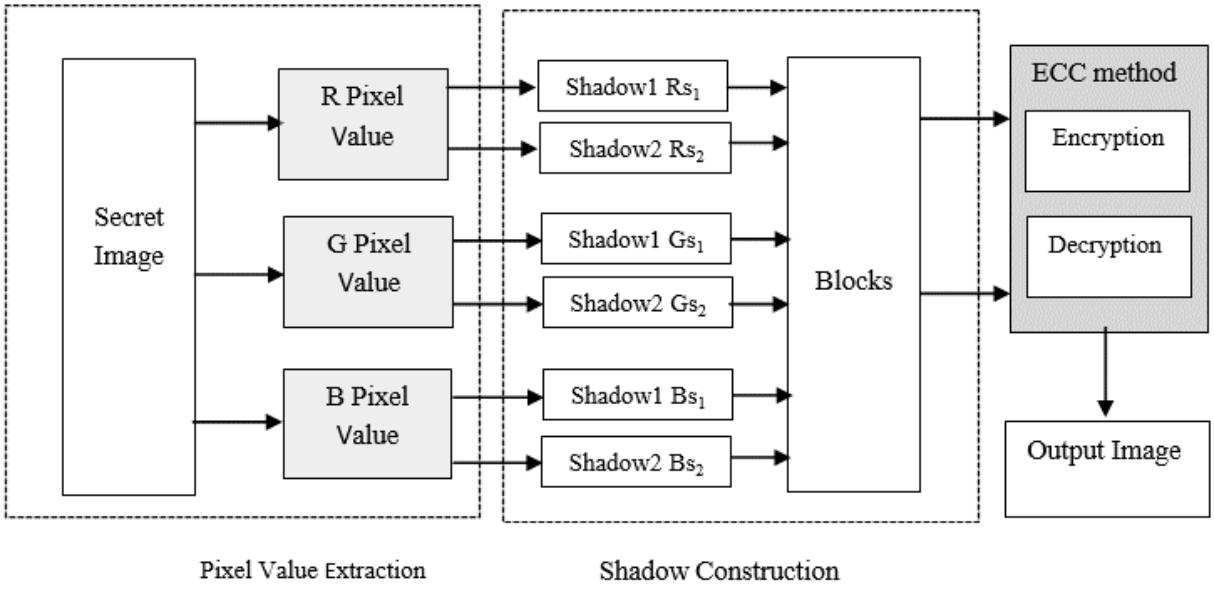

Fig. 4. Propose Scheme of Secret Image Sharing

The encryption procedure commences by introducing a confidential image as the system's input. The image is subjected to a laborious dissection process, wherein its primary color components, namely the red, green, and blue channels, are carefully examined. After being split, individual channels are assigned distinct shadows, which act as a means of representation or alteration to introduce further complexity. Consequently, these distinct shadows are merged to form a cohesive entity, complicating the visibility of the image's initial data. To enhance security measures, a cryptographic algorithm is implemented to encrypt this amalgamated block. Upon reaching the designated moment for image retrieval, a decryption method is utilizedto return the encrypted data to its original condition effortlessly.

Construction Shadow Images

The original image (the secret image) has its RGB values extracted and displayed as three separate matrices (R, G, and B). These matrices, represented by the notation P*Q, share the same dimensions as the source image. There are "n" different variations, or "shadows," of each pixel in the hidden image. Every single cast shadow is made up of smaller RGBA pixels. The pixel values of the original RGB image set each color's shadows. Each component of the RGB color model—red, green, and blue—has its own shadow.

Reconstruction of Shadow Images

The process of shadow reconstruction entails recreating a variety of shadows by employing fundamental XOR operations to produce the initial image. This is done to obtain the original picture. After the shadows have been reconstructed, the ECC method applies the encryption and decryption procedure to each color component. This process is repeated for each shadow. Before encrypting and decrypting the data, the images of each color component are divided into blocks. As the designated block size, the blocks are partitioned into a 4x4 layout configuration.

ECC

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Iss 11, Nov 2022

To use ECC, choose the prime number n_p and the private key H. The cubic equation of an elliptic curve is then,

$$E=p(i))^3+ u*p(i)+v \quad (1)$$

Here, u and v are the constants

The optimal point for the elliptic curve X and Y are chosen if X=Y.

$$X=mod(E,n_p) \quad (2)$$

$$Y=mod((p(j))^2,n_p) \quad (3)$$

The elliptic curve points are p(i, j) and the prime number is np. X and Y are calculated by doubling. The nice part is that Pe, Pf, and H are public and private keys. Pf is the public key.

$$P_f=H*P_e \quad (4)$$

Encryption Method

For each image colour channel, a block is produced and encrypted again. The total number of blocks is b(i, j), where i and j are the block's row and column in the colour component image. Encrypting every pair of successive data is used. The data Dx(i, j) and Dy(i+1,j) and point are:

$$C_1= H*P_e \quad (5)$$

$$C_2=(D_x,D_y)+C_1 \quad (6)$$

Decryption Method

The message is decrypted using the private key (H) during decryption. Point C_{11} is utilized for the decryption of the pixel point.

$$C_{11}=H*C_1 \quad (7)$$

$$C_{ij}=C_2-C_{11} \quad (8)$$

The$C_{ij}$is the output.

Each pixel value is parsed from the Cij output and reconstructed with its original red, green, and blue channels.The encrypted image is recovered at last as

$$F_{image}=\sum(RGB) \quad (9)$$

5. Results and Discussion

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **Volume 11, Iss 11, Nov 2022**

To determine the total number of shadows, we make use of several different visual representations, including image1 (which depicts Lena), image2 (which depicts a house), image3 (which depicts peppers), and image4 (which depicts a baboon). Due to the multiple shadow design, each component has four unique shadows.

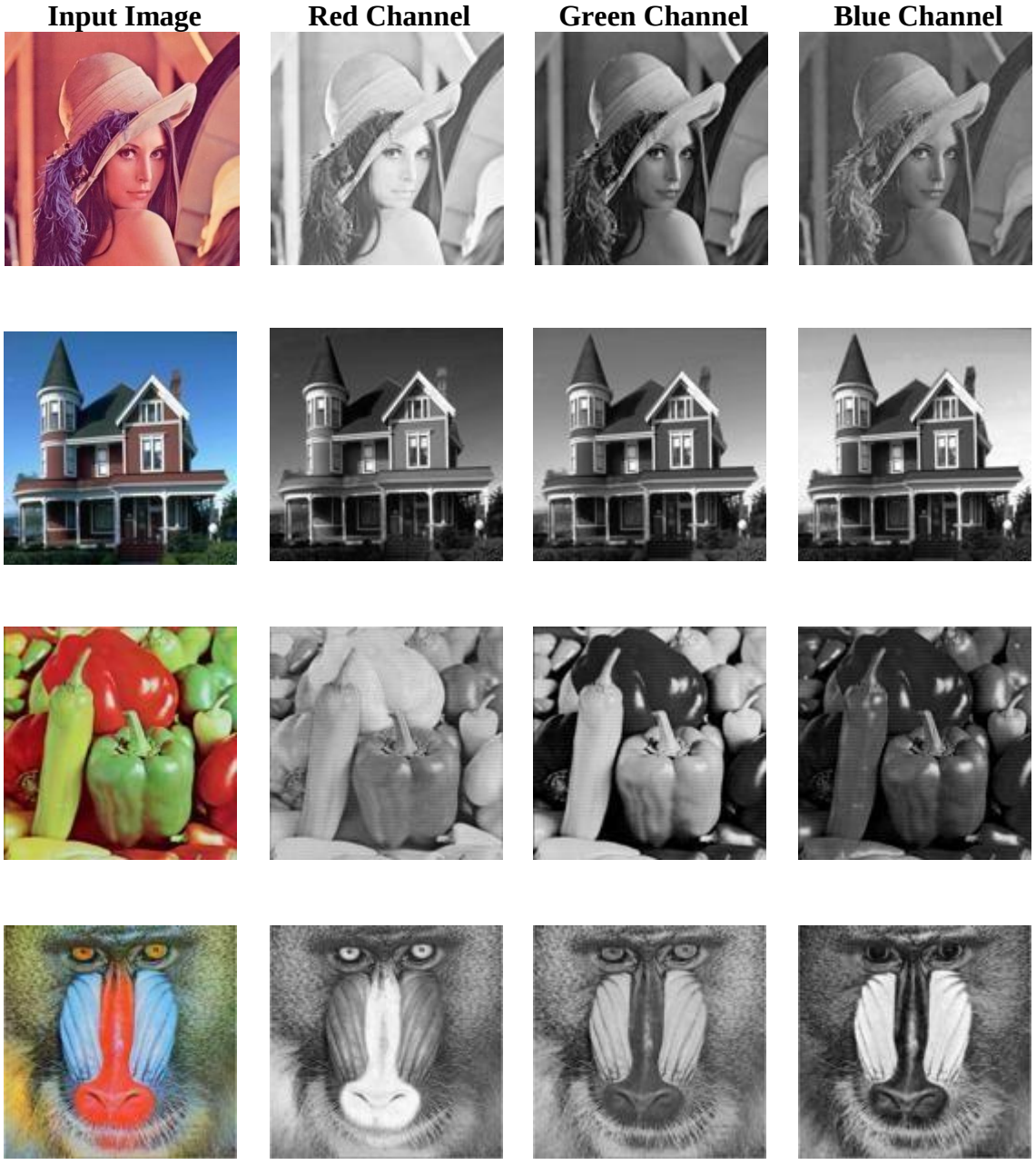

Fig.5. Numerous Images considered for Image Encryption (Red, Green, Blue) channels.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **Volume 11, Iss 11, Nov 2022**

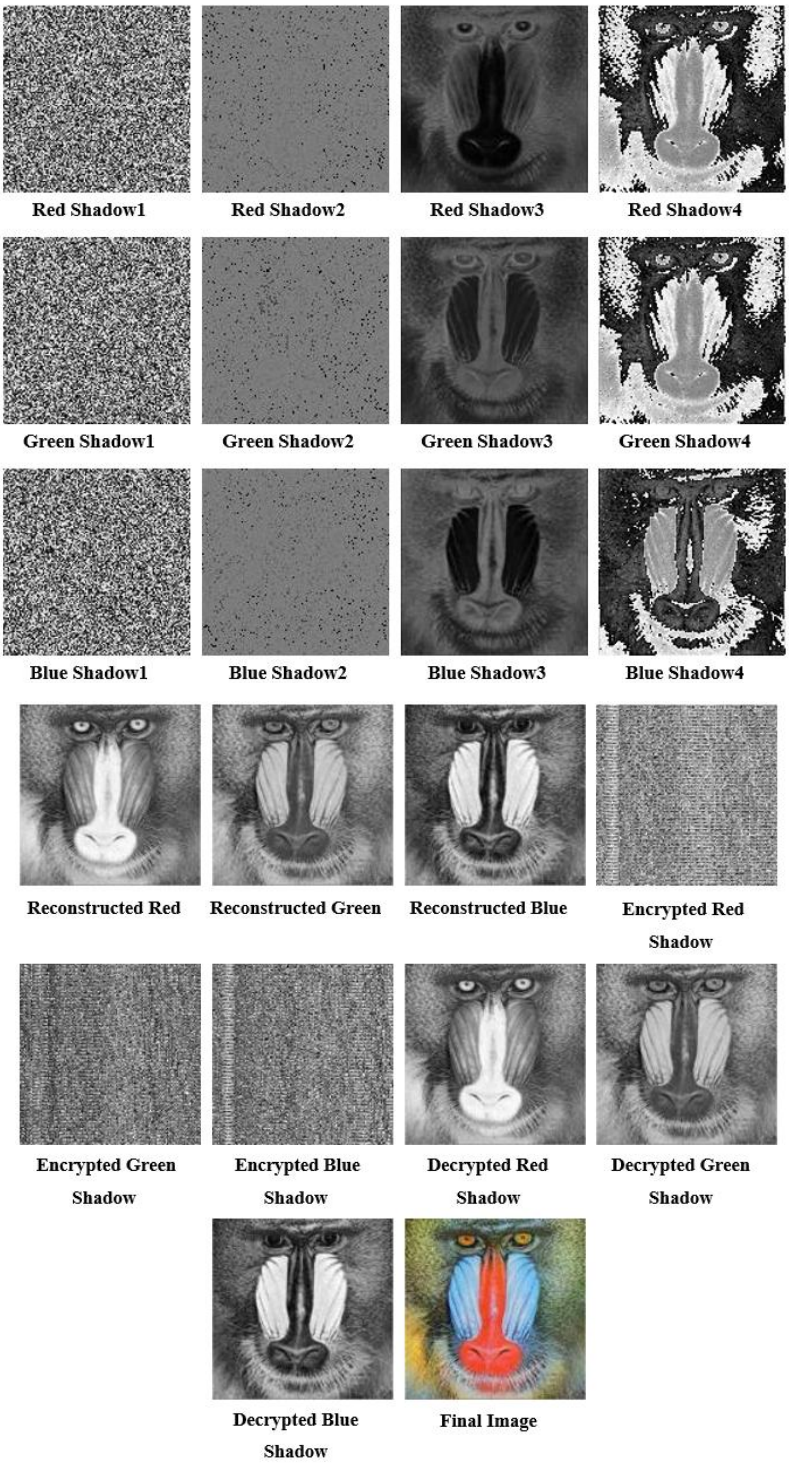

Fig. 6. The proposed work, as demonstrated experimentally on a single image

The method of producing a large number of shadows, which was discussed previously, is used to deduce the shadows. The representations of the initial input image shown in Figure 4 include the image composed of the RGB components and the corresponding shadow images. Metrics such as PSNR, MSE, and CC values are utilized to evaluate the performance of the given method. An innovative attack strategy referred to as the "Pixel Positions Changing Attack" is used in this investigation to evaluate how effective the proposed scheme is. For our investigation, we chose four photos representative of benchmark datasets. In our presentation, we have drawn particular attention to the processing results obtained for the image containing a baboon. Fig. 5 demonstrates the four images with red, green, and blue channels.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **Volume 11, Iss 11, Nov 2022**

In the current study, Fig. 6 depicts the encryption and decryption operations for a sample image labeled "Baboon" using the proposed method. This figure most likely includes side-by-side comparisons or a step-by-step visualization to help readers understand how the "Baboon" image gets converted from its original state to an encrypted format and then back again after decryption. Moving on, Fig. 7 shows the histograms of the Baboon image, which provides insight into the distribution of pixel values. A histogram for an image gives useful information about the frequency distribution of its pixel intensities, revealing information about its contrast, brightness, and overall tonal distribution.Furthermore, Table 1 compares key metrics — PSNR (Peak Signal-to-Noise Ratio), MAP (Mean Absolute Percentage), and CC (Correlation Coefficient) — across four different images. These measurements are critical in determining the encryption and decryption operations' quality, correctness, and dependability. A greater PSNR, for example, usually implies that the decrypted image is of excellent quality, with less distortion or noise than the original. Similarly, MAP and CC values provide information about the decrypted images' correctness and correlation with their original counterparts.

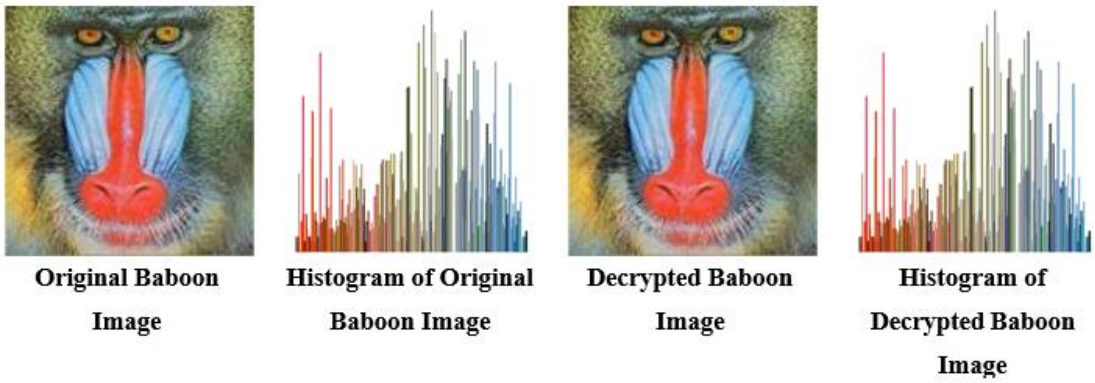

Fig. 7. Histograms of Baboon Image

Table 1. The Evaluation Measures on Four different images

Originalimage	PSNR	MAP	CC
Lena	59.00	0.102	0.98252
House	58.32	0.125	0.98125
Peppers	57.36	0.165	0.98415
Baboon	57.26	0.100	0.97856

Finally, Fig. 8 provides a graphical representation of the results for individuals who prefer a more visual interpretation of data. This could take the shape of bar graphs, line charts, or any other graphical tool that allows readers to easily detect and analyze the efficiency of the proposed strategy when applied to diverse photos. It is important to point out that our judgment was not restricted to only the picture of the baboon. We performed exhaustive computations on various assessment metrics for each of the four photos. Following that, we gave a comparative study based on these metrics, highlighting the differences and similarities between the outcomes for each image.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Iss 11, Nov 2022

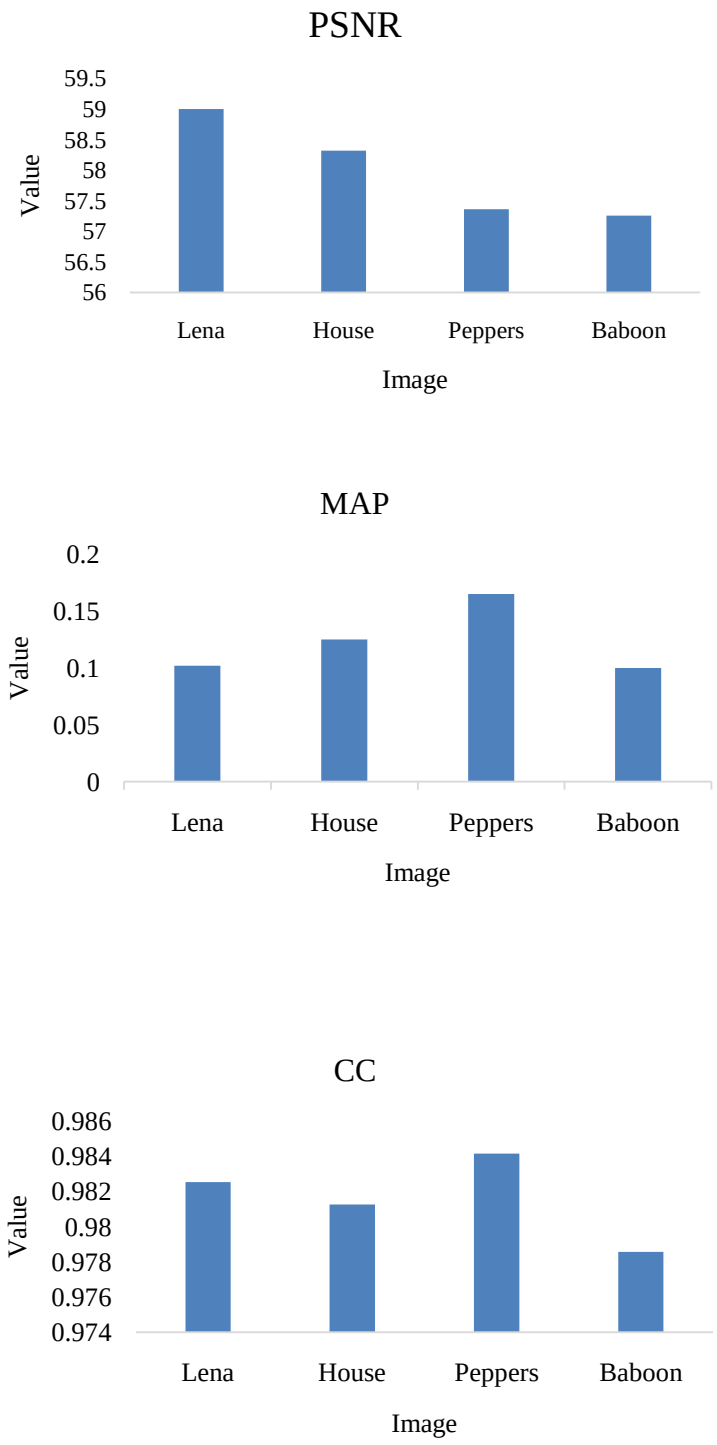

Fig. 8. Comparison results of four different images (PSNR, MAP,and CC)

6. Conclusion

The employment of elliptic cryptography in the system for sharing secrets has shown remarkable performance, as evidenced by numerous shadows in this ground-breaking method. This discovery was made possible because elliptic cryptography was utilized. The process produces a large number of irrational shadows, each of which may be efficiently encoded and decoded using the encryption and decryption methodology aligned with ECC. The P.S.N.R. values of 59, 58, 57, and 59 show that the image quality is still quite high despite hidden elements. All of the correlation coefficient values

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **© 2012 IJFANS. All Rights Reserved**, Volume 11, Iss 11, Nov 2022

point toward a positive link, and they are getting closer and closer to having a value of 1. The pictures also have mean square errors of 0.10, 0.1176, 0.1454, and 0.0997. Since the pixels are not randomly selected, the suggested method preserves the initial image's quality. The investigation of correlation coefficients and histogram estimations has produced indisputable proof that encryption is utilized on sensitive imagesto protect the confidentiality of the image.

REFERENCES

1. Saba, S. J., Al-Nuaimi, B. T., & Suhail, R. A. (2023, March). A review of traditional, lightweight, and ultra-lightweight cryptography techniques for IoT security environment. In *AIP Conference Proceedings* (Vol. 2475, No. 1). AIP Publishing.
2. Zhang, F., Guo, Y., Pu, M., Chen, L., Xu, M., Liao, M., ... & Luo, X. (2023). Meta-optics empowered vector visual cryptography for high security and rapid decryption. *Nature Communications*, *14*(1), 1946.
3. Yan, Y. (2022, December). The Overview of Elliptic Curve Cryptography (ECC). In *Journal of Physics: Conference Series* (Vol. 2386, No. 1, p. 012019). IOP Publishing.
4. Astorga, J., Barcelo, M., Urbieta, A., & Jacob, E. (2022). Revisiting the feasibility of public key cryptography in light of IoT communications. *Sensors*, *22*(7), 2561.
5. Yan, Y. (2022, December). The Overview of Elliptic Curve Cryptography (ECC). In *Journal of Physics: Conference Series* (Vol. 2386, No. 1, p. 012019). IOP Publishing.
6. Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography: Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*, 100530.
7. Pandey, K., & Sharma, D. (2023, June). Advances in data security through elliptical curve cryptography. In *AIP Conference Proceedings* (Vol. 2819, No. 1). AIP Publishing.
8. Bao, J. (2022, April). Research on the security of elliptic curve cryptography. In *2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)* (pp. 984-988). Atlantis Press.
9. Ye, G., Liu, M., & Wu, M. (2022). Double image encryption algorithm based on compressive sensing and elliptic curve. *Alexandria Engineering Journal*, *61*(9), 6785-6795.
10. Dawahdeh, Z. E., Yaakob, S. N., & bin Othman, R. R. (2018). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University-Computer and Information Sciences*, *30*(3), 349-355.
11. Nagaraj, S., Raju, G. S. V. P., & Rao, K. K. (2015). Image encryption using elliptic curve cryptography and matrix. *Procedia Computer Science*, *48*, 276-281.
12. Abd El-Latif, A. A., & Niu, X. (2013). A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-International Journal of Electronics and Communications*, *67*(2), 136-143.
13. Singh, L. D., & Singh, K. M. (2015). Image encryption using elliptic curve cryptography. *Procedia Computer Science*, *54*, 472-481.
14. Liu, Z., Xia, T., & Wang, J. (2018). Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes–Vanstone elliptic curve cryptosystem. *Chinese Physics B*, *27*(3), 030502.
15. Obaid, Z. K., & Al Saffar, N. F. H. (2021). Image encryption based on elliptic curve cryptosystem. *International Journal of Electrical and Computer Engineering*, *11*(2), 1293.
16. Bashir, Z., Malik, M. A., Hussain, M., & Iqbal, N. (2022). Multiple RGB image encryption algorithms based on elliptic curve, improved Diffie Hellman protocol. *Multimedia Tools and Applications*, *81*(3), 3867-3897.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **Volume 11, Iss 11, Nov 2022**

17. Ibrahim, S., & Alharbi, A. (2020). Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. *IEEE Access*, *8*, 194289-194302.
18. Azam, N. A., Ullah, I., & Hayat, U. (2021). A fast and secure public-key image encryption scheme based on Mordell elliptic curves. *Optics and Lasers in Engineering*, *137*, 106371.
19. Jasra, B., Saqib, M., & Moon, A. H. (2021, April). Mapping images over elliptic curve for encryption. In *2021 6th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.
20. Singh, K. M., Singh, L. D., &Tuithung, T. (2023). Improvement of image transmission using chaotic system and elliptic curve cryptography. *Multimedia Tools and Applications*, *82*(1), 1149-1170.