Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

Image Encryption using Elliptic Curve Cryptography with Data Security

Ms. Silpa K. S.
Assistant Professor
Department of Computer Science
College of Applied Science, Nattika

Ms. Rameela Ravindran K.
Assistant Professor
Department of Computer Science
St. Thomas' College (Autonomous), Thrissur

***Abstract*— With the advent of Internet and associated technologies millions of data in the form of text and images are transferred everyday across the network. It is essential to ensure confidentiality and integrity the data being transferred. Cryptography and Steganography plays a significant role in transferring images securely. The exponentially hard problem to solve an Elliptic Curve Discrete Logarithm Problem makes the technique secure even with a smaller size key compared to other cryptographic techniques. In this paper, author implement the Elliptic Curve cryptography to encrypt, decrypt and use Sequential Color Cycle Algorithm to steganograph the data to provide additional data security.**

Keywords*— *ECC- Elliptic Curve Cryptography; DLP- Discrete Logarithemuc Problem; Digital signature; Elliptic curve discrete logarithm problem; Authenticity; Integrity. Stegenography, Data security, SCCA -Sequential Color Cycle Algorithm.

I. INTRODUCTION

In today's era of communication, data transfers is a common phenomenon. Data can be in the form of audio, video, text or images. When the data to be transferred is confidential then arises the problem of secure data transfer techniques. Security of data can be enhanced by using techniques like cryptography, steganography on data to be transferred. The cryptographic technique which we have implemented in this paper is the Elliptic Curve Cryptography (ECC). Various study on ECC has concluded that the difficultly to solve an Elliptic Curve Discrete Logarithmic Problem(DLP) is exponentially hard with respect to the key size used. This property makes ECC a very good choice for encryption/decryption process compared to other cryptographic techniques which are linearly difficult or sub exponentially difficult. ECC is a public key cryptography which was developed by Neal Koblitz and Victor S. difference [1,2] independently in the year 1985. ECC gains wide acceptance around 2004. Steganographic technique used in this paper is Sequential Color Cycle Algorithm[12].

Elliptic Curve Basic Operations:
Elliptic curve basic operations include point addition, point subtraction, point multiplication and pointdoubling.

Point Addition:
Point Addition defines addition of two points P and Q using elliptic curve equation to obtain another point R, *i.e.,* R = P + Q. Suppose $P(x_1,y_1)$ and $Q(x_2,y_2)$ are points on elliptic curve. If $x_1=x_2$ and $y_1=-y_2$, then P+Q= θ (point at infinity). Otherwise P+Q = (x_3,y_3) = R where
$x_3 = s^2 - x_1 - x_2 \bmod p$
$y_3 = s(x_1 - x_3) - y_1 \bmod p$, and

$$s = \begin{cases} [(y_2 - y_1)/(x_2 - x_1)] \bmod p, & \text{for } P \neq Q \\ [(3x^2 + a)/2y_1] \bmod p, & \text{for } P = Q \end{cases}$$

Geometric explanation to point addition:
Let P and Q be two distinct points on an elliptic curve, and P is not equal to -Q. Draw a line through the two points and this line will intersect the elliptic in exactly one more point, call -R. This point is reflected along the x-axis to get the point R.

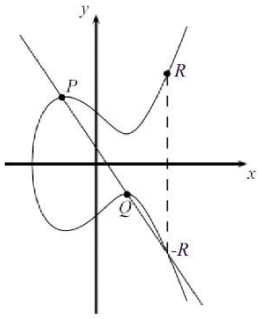


Figure 1(a)

Point Subtraction:
Point Subtraction defines subtraction of two points P and Q using elliptic curve equation to obtain another point R, *i.e.,* R = P - Q. Suppose $P(x_1,y_1)$ and $Q(x_2,y_2)$ are points on elliptic curve.
To perform point subtraction, get a mirror coordinate of the subtracted point $Q(x_2,y_2)$ along x-axis and then perform point addition on the resulting coordinate $Q(x_2,-y_2)$ and the other coordinate P.
Geometric explanation to point subtraction:
Let P and Q be two distinct points on an elliptic curve. Draw a line through the two points and this line will intersect the elliptic in exactly one more point, call -R. This point is reflected along the x-axis to get the point R.
$P(x_1, y_1) - Q(x_2, y_2) = P(x_1, y_1) + Q(x_2, -y_2)$

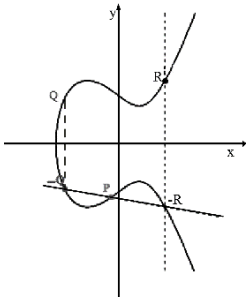


Figure 1(b)

Point multiplication:
Point Multiplication is the repeated addition of the given point. kP = P + P + P +· · ·+k times.
Point Doubling:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

Point Doubling defines addition of a point P to itself using elliptic curve equation to obtain another point R,
i.e. R = 2P.
Geometric explanation to point doubling:
To add a point P to itself, a tangent line to the curve is drawn at the point P. It intersects the elliptic curve exactly at one other point-R. -R is reflected in the x- axis to get R. This operation is called the point doubling.

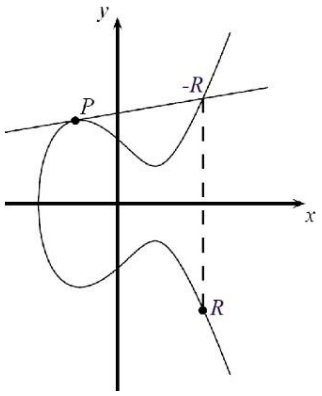


Figure 1(c)

The Discrete Logarithmic Problem
The security due to ECC relies on the difficulty of DLP in elliptic fields. If P and Q are two points on any elliptic curve, so that Q = kP, where k is a scalar, then it is easy to obtain Q when we know k and P but hard to know k even if we know P and Q as k should be large. This k is the discrete logarithm of Q to the base P.
Encryption and decryption using ECC
Let Alice and Bob be the two communicating party. The communicating parties agrees upon the Elliptic curve equation and a Generator (G).
$y^2 = \{x^3 + ax + b\} \bmod [p]$
Suppose Alice want to encrypt a message 'Pm' and send to Bob. The cipher text is given by Pc = [kG, Pm + kPb]where 'k' is a random integer and 'Pb' is the public key of Bob computed using the private key of Bob 'nB', Pb =nBG. Bob decrypts the cipher message as, message = [Pm + kPb − nBkG]. Since Pb = nBG, kPb and nBkG cancel each other and 'Pm' remains, which is the message sent by Alice.

II. LITERATURE SURVEY:

Since from the earlier times, people are bothered about how to securely transmit secret messages. Both cryptographic techniques and steganographictechniques are used to achieve this aim. In cryptography, the existence of the encrypted message is visible to the world, whereasin steganography, only the sender and the receiver know the existence of the message. Darrel Hankerson, Alfred Menezes, and Scott Vanstone[3] explained the various arithmetic behind elliptic curves and addressessome issues that arise in ECC implementation in detail. Lawrence C. Washington[4] provides an introduction to both the number theoretic and the cryptographic sides of elliptic curves. To securely transfer text and image through the network, various techniques have been developed in recent years using Elliptic Curve Cryptography. S. Maria Celestin Vigila and K. Muneeswaran[5] proposed an image encryption algorithm using ECC. They generated the values of k and nB by a random number generator, Comparative Linear Congruential Generator (CLCG) to give credibility. Ali Soleymani, Md Jan Nordin, and Zulkarnain Md Ali[6] creates a mapping table which has the intensity values ranging from 0 to 255 along the row and the corresponding columns of each row contain the elliptic curve coordinates. All the pixels of an image are mapped to related points on the elliptic curve using the table and encryption is done using receiver's public key. To view the cipher image, we refer to the mapping table and find the current index according to each point and replace with the related value. Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh[7] proposeda technique using ECC which works on the group of pixels to reduce the number of computations. This technique helps to ignore the mapping operation of each pixel into elliptic curves and the need to share mapping table between sender and receiver. Shailender Gupta, *et. al.* [8] proposed a scheme in which the encrypted information is converted into binary form and embedded in the LSB of image pixels, which is also in the binary form. M.Sivaram, *et. al.* [9] presents a new method in which the secret image is embedded into the cover image in the last two positions of the LSB at random pixels. This technique overcomes the problems faced by the steganographic techniques like 1-bit LSB. Mekha Jose[10] proposes an LSB steganographic technique of 3-bit data hiding method. In this technique, the secret image bits are taken 3 at a time. Each of the 3 bits of the secret image is embedded into last 3 LSB bits of cover image pixels. Parisa Gerami, *et. al.* [11] proposed a four-step method for image steganography.It increases the quality of stego-image. The secret and cover images are transformed first and then reshuffles the secret image based on Wu's et al. method. After this, the secret image is embedded into 4 bit LSB of the cover-image. Finally, it applies optimal pixel adjustment (OPA) on stego-image. Lip Yee Por, *et. al.*
[1] gave a detailed idea of a steganographic scheme which employs sequential colour cycle algorithm. They proposed an algorithm which combines one bit, two, three, four bits LSB steganography and colour cycle steganography. By using this algorithm, the entire LSBs are fully utilised to encode secret data of each pixel sequentially after being converted into the binary string. Therefore, different types of data files can be embedded in cover images as secret data.

III. PROBLEM STATEMENT

In elliptical curve cryptography it is necessary to use a mapping table to map the pixel values to the elliptical curve coordinates. But by using grouping of pixels and converting it a single large integer such that it is less than 'p', a parameter of the elliptical curve equation offinite field, and hence reduce the computational time and also the overhead to share the mapping table for decryption[7]. But here also the 'kG' has to be sent to the receiver to decrypt the image or text. In our algorithm, we embed data on the cipher image using Sequential Color Cycle Algorithm[12].

IV. PROPOSED ALGORITHM

In this proposed algorithm, grouping of pixels is done to reduce the computation steps in ECC [7]. To add further, data may be embedded inside each group during encryption. This helps to enhance the capacity of data being embedded. The resultant cipher image may be further embedded with the 'kG' value which is required for decryption. To avoid intruder's unwanted attention the image is embedded into any cover image.
Data embedding inside image:
1. Convert the data into binary format.
2. Get the pixel value of the cover image
3. For each bit in the binary string to beembedded
i. Adjust the difference in values of the adjacent pixel RGB components to embed data bit.
ii. Move to the next RGB component.
iii. Move to the next pixel after cycling though

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

RGB

Image encryption

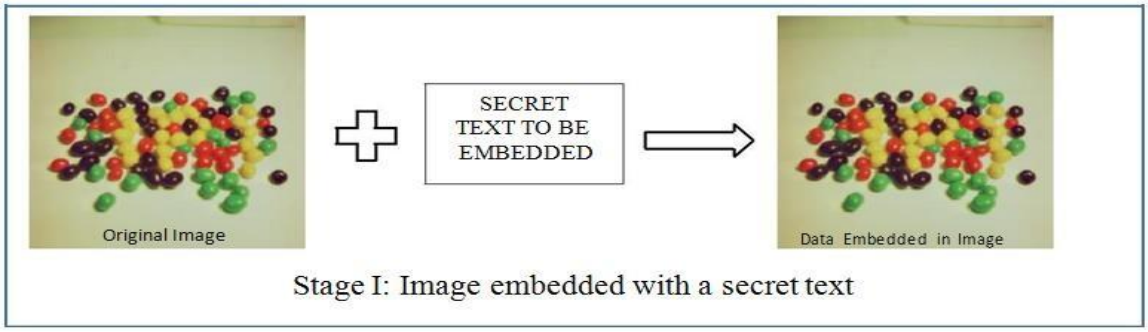
1. Get the pixel value of the image to be encrypted. Record the number of channels present in the image.
2. Group the pixels and convert to single large integer value for each group using function FromDigits [list of pixels, b] which take a list of pixels and convert it to base b usually taken as 256.
3. Number of pixel in each group is given by *grp* = Length [IntegerDigits[p, 258]] – 1
IntegerDigits [big integer value, 256] takes as input the big integer values in the rangeof the size chosen for ECC operation and with base 256, the output will be a list of values ranging from 0 to 255.
4. Pair up the result obtained from step 3 and store as '*Pm*' which is the plain message input for the ECC system.
5. Generate a random '*k*' and compute '*kG*' and '*kPb*' where '*Pb*' is the public key of the receiver.
6. Perform point addition of '*kPb*' with each value of '*Pm*' and store as '*Pc*' which is the cipher text.
7. Convert the cipher text list from step 6 to value ranging from 0 to 255 using function defined in step 3.
8. Pad left with 0 to each list from step 7 which have less than *grp* + 1 number of elements, to make each list equal in length. Flatten the list from step 8, group them according to the number of image channels recorded and partition them to width of the plain image.
9. Convert the values from step 8 into cipher image

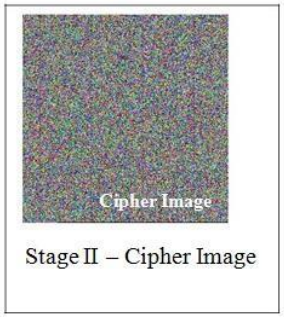
Image Decryption

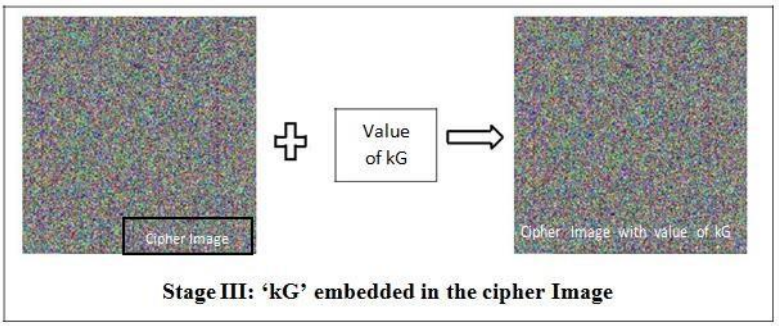
1. Get the pixel value of the cipher image and group by *grp* + 1 number of pixels and form single big integer value for each group with base 256. Record the number of image channels of the cipher image.
2. Pair up the value obtained from step 1.
3. Perform point multiplication of '*kG*' with '*nB*' where '*nB*' is the private key of the receiver.
4. Perform point subtraction between values from step 2 with value from step 3.
5. Get the value in the range of 0 to 255 from step 4 with base 258 and subtract random 2 from each value.
6. Group the flatten value obtained in step 5 in term of recorded number of image channels of the cipher image and partition them to the width of thecipher image.
7. Convert the values from step 6 into plain image.

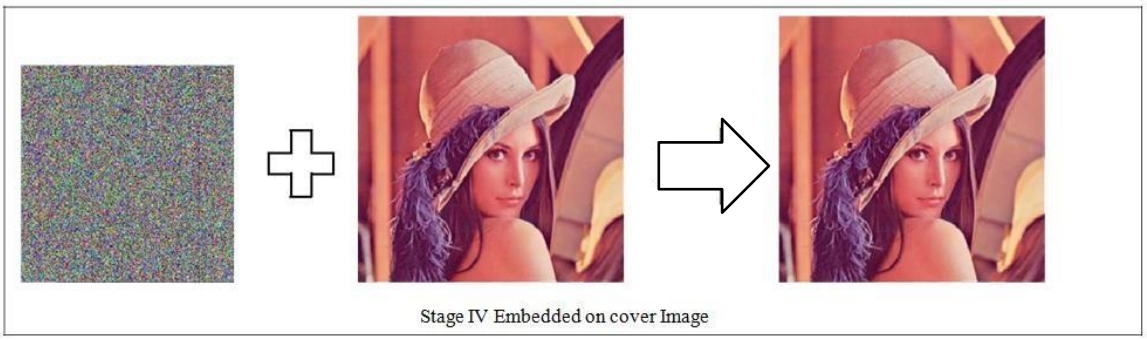
Data retrieval from image:

1. Get the pixels of the cover image
   i. Retrieve the data bit from the cover image as the difference between the adjacent RGBcomponents
   ii. Move to the next RGB component.
   iii. Move to the next pixel after cycling though RGB
2. Append each bit stripping out the delimiters









International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

V. SECURITY ANALYSIS

Security analysis of a cryptographic process and steganographic is an essential process to ensure the stealth of the cryptographic and steganographic technique. In this section we discuss some analysis of the implemented technique:

Histogram analysis:

Histogram of an image depicts the frequency of each pixels. A good cipher image has a uniform frequency distribution of the pixel values. Figure 2(a), 2(b) depicts the histogram of the plain image, cipher image (with data embedded in it).

Key space: The bigger the key size, more difficult it is to perform an attack using Brute Force attack. ECC provides an exponentially difficult Elliptic Curve Discrete Logarithmic Problem with respect to the key size. The key used in this implementation is quite large.

Key sensitivity: In the technique key is highly sensitive to the extent that a slight change in original key should give a drastic change in the recovered image obtained from the cipher image. Figure 3(a), 3(b) and 3(c) represent original image, cipher image with data embedded, and decrypted image with original key respectively. Figure 3(d) image decrypted with key changed by a single digit.

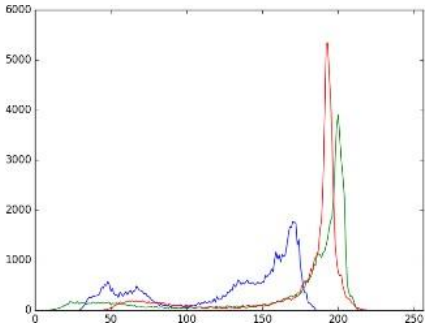


Figure 2(a)

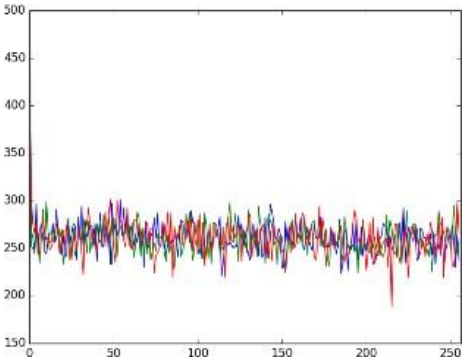
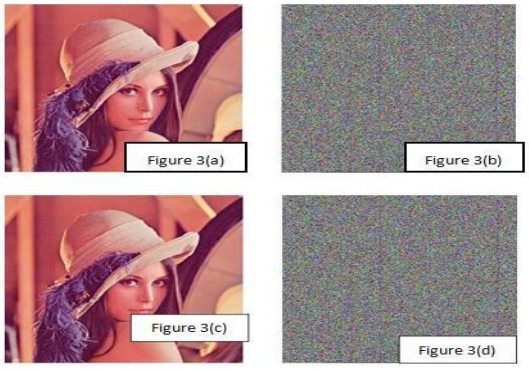


Figure 2(b)



Entropy analysis: Entropy is the measure of degree of randomness. Image encryption requires cipher image pixel values to be highly random. Table 1 depicts the entropy analysis.

Table 1: Entropy analysis

Image	Size	Entropy
Lena	512*512	7.99865792765
Peppers	256*256	7.99887651549

Stego-Image Distortion Analysis: Peak Signal-to- Noise Ratio (PNSR) is used to measure the quality of the stego-image that produced by steganographic tool. PNSR is a metric to measure the distortion between an original image and a reconstructed image.For the proposed algorithm the PSNR ratio is 47 dB.

Capacity Analysis: Embedding capacity of the payload refers to the length of the secret data which can be embedded into a coverimage.

VI. CONCLUSION

In the paper we have presented the implementation technique of secure data transfer by using image encryption/decryption and steganography to embed data cipher image. The image may be embedded with a text/image before encryption and the value 'kG' may be embedded on the cipher image for easy transfer. Also since the cipher image is embedded on a cover image it create a stealth camouflage to avoid intruder's unwanted attention. The proposed algorithm providesa two security shield to the text/data embedded in the image ensuring data security. Further work will focus on including a watermark on the cipher image thus ensuring data authorization and authentication.

VII. REFERENCES

[1] Koblitz, N., Elliptic Curve Cryptosystems. *Mathemathics of Computation*vol. 48 pp. 203- 209,(1987)

[2] Miller, V., Use of Elliptic Curves in Cryptography. In: Advances in Cryptology - Crypto '85. *Lecture Notes in Computer Science*, Vol. 218. Springer-Verlag, pp. 417-426, (1986)

[3] Darrel Hankerson, Alfred Menezes and Scott Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, (2004).

[4] Lawrence C. Washington, *Elliptic Curves Number Theory and Cryptography*, Taylor & Francis Group, Second Edition, (2008).

[5] S. Maria Celestin Vigila and K. Muneeswaran, Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications, In *International Journal of Network Security*, vol. 14, no. 4, pp. 236–242, July (2012).

[6] Ali Soleymani, Md Jan Nordin and Zulkarnain Md Ali, A Novel Public Key Encryption based on Elliptic Curves Over Prime Group Field, In *Journal of Image and Graphics*, vol. 1, pp. 43– 49, (2013).

[7] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, Image Encryption using Elliptic Curve Cryptography, In Eleventh International Multi-Conference on Information Processing- 2015 (IMCIP-2015)

[8] Shailender Gupta, Ankur Goyal and BharatBhushan, Information Hiding Using LeastSignificant Bit Steganography and Cryptography, *I.J.Modern Education and Computer Science*,2012, 6, 27-34 Published Online in MECS(http://www.mecs-press.org/)DOI: 10.5815/ijmecs.2012.06.04 (2012)

[9] M.Sivaram, B.Durga Devi, and J.Anne Steffi, Steganography of two LSB Bits, *International Journal of Communications and Engineering Volume 01– No.1, Issue: 01 March2012*

[10] Mekha Jose, Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Impact Factor (2012): 3.358

[11] Parisa Gerami, Subariah Ibrahim, and Morteza Bashardoost, Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment, *International Journal of Computer Applications (0975 – 8887) Volume 55– No.2, October 2012*

[12] Lip Yee Por, Delina Beh, Tan Fong Ang and Sim Ying Ong, An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm, *The International Arab Journal of Information Technology, Vol. 10, No. 1, January 2013*