www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC
Gestão, Inovação e Tecnologias

ECC Data Hide – Using Steganoraphy and Deep Neural Network

Dr.V. Vennila[1]; L.I. Poomani[2]; S. Thaaranya[3]

[1]Associate Professor, Department of CSE, K.S.R College of Engineering, Tiruchengode, India.
[2]Final Year Student, Department of CSE, K.S.R College of Engineering, Tiruchengode, India.
[3]Final Year Student, Department of CSE, K.S.R College of Engineering, Tiruchengode, India.

Abstract
In the field of computer networks, cryptography and steganography are the well-known features for best security purpose. The main idea is to transmit the data securely. So, providing acceptable level of security is essential for data transmission. Also it should reduce the time complexity of the security algorithm. Here we have employed the "Elliptic Curve Cryptography" scheme to encrypt the data and image. A "Least Significant Bit" steganography algorithm is used to insert the encrypted data to be hidden inside the image in order to send the data securely. The encrypted data from the image is then decrypted by the decryption algorithm. Finally the hidden data is taken from the decrypted data. Then the image is compressed before sending through the internet. MATLAB is utilized to mimic outcomes which show that it has great inserting limit and security.

Key-words: Elliptic Curve Cryptography, Least Significant Bit, Deep Neural Network.

1. Introduction

1.1. Elliptic Curve Cryptography

Elliptic bend cryptography (ECC) is a way to deal with public-key cryptography method dependent on the mathematical design of elliptic bends over limited fields. Elliptic bend cryptography requires more modest keys when contrasted with non-Elliptic bend cryptography to give identical security when contrasted with different calculations and strategies. Elliptic bends are relevant for key age, advanced marks, pseudo-irregular key generators and different errands. In a roundabout way, they can be utilized for encryption by joining the critical concurrence with an uneven encryption conspire. They are likewise utilized in a few whole number factorization calculations dependent on

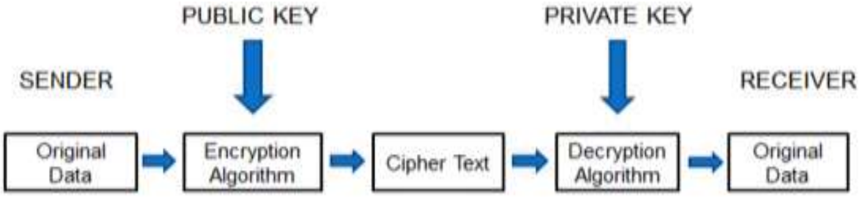
Received: 03.03.2021 – Accepted: 08.04.2021

elliptic bends that have applications in cryptography technique, for example, Lenstra elliptic-bend factorization.

1.2. Block Diagram Of ECC

From the square chart Figure 1.1, the message is being sent from the sender to the beneficiary. At that point the message is covered up into the LSB of the picture. This strategy is finished by utilizing the LSB steganography. Here, first the ASCII estimation of the content is known and afterward it is changed over into the double worth. In the subsequent stage the content is inserted into the LSB of the picture. The public key of the collector is known to the sender. The first message is being encoded utilizing the beneficiaries public key with the assistance of encryption calculation. The encryption is finished by utilizing the Elliptic bend cryptography. The first message is then changed over into the code text which is the scrambled message. The encoded message is then decoded by utilizing the recipients private key which coordinates with the collectors public key. The unscrambling is then done by utilizing the Elliptic bend cryptography. The content is then being taken from the LSB of the picture.

Figure 1.1- Block Chart of ECC



1.3. Steganography

Steganography is the method of concealing restricted information inside a common, non-mystery, record or message to maintain a strategic distance from discovery; the restricted information is then separated at its objective. The utilization of steganography can be joined with encryption as an additional progression for stowing away or securing information. The word steganography is gotten from the Greek words steganos and the Greek root chart Steganography can be utilized to cover practically any kind of computerized content, including text, picture, video or sound substance; the information to be covered up can be covered up inside practically some other sort of advanced substance. The substance to be disguised through steganography called covered up text is frequently encoded prior to being joined into the harmless appearing cover text document or information stream. If not encoded, the secret content is usually prepared here and there to expand the trouble of recognizing the mysterious substance.

2. Literature Review

K. Muhammad [5] examined that computerized steganography is a sprouting research region that utilizes advanced pictures, recordings, network conventions, and sound for data disguise. From the most recent decade, a few methodologies for computerized steganography have been proposed in the spatial area. These methodologies depend on LSB replacement, edge based implanting, and pixel pointer based installing. In this part, we present a short outline of the essential LSB strategy and talk about some other existing cutting edge strategies inside every class that are identified with the proposed technique. Toward the finish of this part, we present a few procedures to adapt up to the restrictions of the techniques referenced.

Laiphrakpam Dolendro Singh et al [4] suggested that large number of pictures are moved ordinarily across the organization. A portion of these pictures are classified and we need these pictures to be moved safely. Cryptography assumes a huge part in moving pictures safely. The dramatically difficult issue to settle an Elliptic Curve Discrete Logarithm Problem concerning key size of Elliptic Curve Cryptography, helps in furnishing a significant degree of safety with more modest key size contrasted with other cryptographic method which relies upon whole number factorization or Discrete Logarithmic issue. In this paper, we execute the Elliptic Curve cryptography to scramble, decode and carefully sign the code picture to give realness and uprightness.

Ahmed An et al [7] proposed a strategy to safely move picture across the organization different methods have been create lately utilizing ECC. They introduced a picture encryption method utilizing cyclic elliptic bend. They proposed a procedure to produce a pseudo irregular key stream utilizing cyclic elliptic bend point which thusly is utilized for encryption of information stream. They tracked down that known-plain content assault and picking a plain picture with all the pixel esteem 0 can produce the scrambled picture.

Jayati Bhadra et al [2] clarified that steganography is a technique for concealing mystery messages in a cover object while correspondence happens among sender and recipient. Security of private data has consistently been a significant issue from the past occasions to right now. It has consistently been the intrigued point for analysts to create secure methods to send information without uncovering it to anybody other than the recipient. In this manner occasionally analysts have created numerous methods to full fil secure exchange of information and steganography is one of them. In this paper we have proposed another strategy of picture steganography for example Hash-LSB with RSA calculation for giving greater security to information just as our information concealing technique. The proposed strategy utilizes a hash capacity to create an example for concealing information bits into LSB of RGB pixel estimations of the cover picture. This method ensures that the message has been scrambled prior to concealing it into a cover picture. In the event that regardless the code text got uncovered from the cover picture, the halfway individual other than collector can't get to the message for what it's worth in scrambled structure.

C.R. Kim et al [3] says that steganography conceals privileged intel in the cover pictures so normally that the presence of covered up information in the stego-picture isn't conspicuous. This Letter proposes another way to deal with dazzle translating of picture steganography utilizing the neighborhood entropy disseminations of decoded pictures. The nearby entropy circulations of inaccurately decoded pictures are not the same as those of ordinary ones as a result of the strange picture structures in the wrongly decoded pictures. This visually impaired disentangling in the picture steganography is valuable to separate secret picture data in light of the fact that there are tremendous least critical piece (LSB)- based steganography techniques, and it is elusive the strategies by noticing controlled LSBs.

Yang Ren-Er et al [8] proposed a strategy to improve the security of steganography, this paper considered picture steganography joined with pre-handling of DES encryption. When sending the restricted data, right off the bat, encode the data planned to stow away by DES encryption is scrambled, and afterward is written in the picture through the LSB steganography. Encryption calculation improves the most reduced coordinating with execution between the picture and the privileged intel by changing the factual qualities of the restricted data to upgrade the counter identification of the picture steganography. The trial results showed that the antidetection power of picture steganography joined with pre-preparing of DES encryption is discovered far superior to the way utilizing LSB steganography calculations straightforwardly.

3. Proposed System

In the proposed technique, the picture is scrambled and decoded by utilizing the elliptic bend cryptography calculation and the most un-huge piece steganography is acted to shroud the content inside the LSB of the encoded picture for greater security reason and recover the content that is covered up in the LSB of the encoded picture by utilizing the unscrambling calculation in the collector side.

3.1. The First and Foremost Step is the Key Generation Module

For information encryption and decoding, we ought to create a public key, secret key and private key to move the information in a safe way. The calculations are given beneath.

3.1.1. User A Key Generation

The sender A chooses an irregular number kA from 1 to n-1.

The sender An at that point produces the public key with the assistance of the equation.

public key P=kA*G

kA - is the sender's private key

G - Generation point

3.1.2 User B Key Generation

The sender B creates the public key with the assistance of the equation.

public key R=kB*G

kB - Receiver's private key

G - Generation point

Secret Key Generation

Secret Key of A, K=kA*R

The Secret key of an is acquired by increasing the private key of An and the Public key of B.

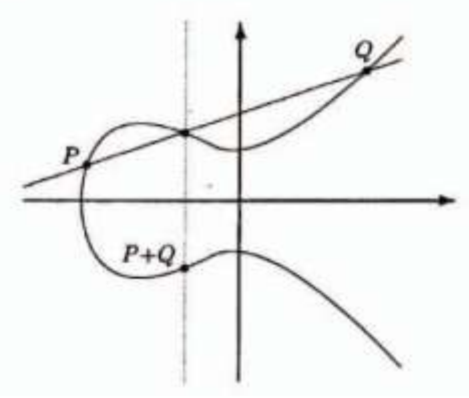
Secret key of B, K=kB*P

The Secret key of B is acquired by increasing the private key of B and the key of A.

3.2. Encryption Module

In this proposition ECC is chosen as an encryption technique. Encryption is finished utilizing a public key, which is of short length. The Figure 4.1 is the normal elliptic bend cryptography bend when the encryption and decoding calculation happens.

Figure 2- ECC Curve



Steps involved with key generation:

1. Select the private key.
2. Get the public key.
3. Send the public key for flow.

Steps involves with encryption part:

1.Select the message to be furtively covered up in a picture.

2. Encrypt the message with the public key and the ECC calculation.

3.3. Image Encryption

The encryption calculation are as per the following

1. Get the pixel estimation of the picture to be scrambled and haphazardly add 1 or 2 to every pixel. Record the quantity of directs present in the picture.
2. Group the pixels and convert to single enormous whole number incentive for each gathering. Number of pixel to be bunch utilizing Mathematica is given by

   grp= Length [IntegerDigits[p, 258]] − 1
3. Pair up the outcome got from stage 2 and store as 'Pm' which is the plain message contribution for the ECC framework.
4. Select an irregular 'k' and register 'kG' and 'kPb' where 'Pb' is the public key of the collector.
5. Perform point expansion of 'kPb' with each estimation of 'Pm' and store as 'Pc' which is the code text.
6. Convert the code text list from stage 5 to esteem going from 0 to 255.

7. Pad left with 0 to each rundown from stage 6 which have not exactly grp+ 1 number of components, to make each rundown equivalent long.

3.4. Decryption Module

Steps engaged with decoding part:

1. Get the content installed picture.
2. Resize the picture.
3. Separate the message by finding the LSBs to get back the encoded message.
4. Decrypt the message with the private key and ECC calculation.

3.5. Steganography

Steganography is the way toward concealing the content inside the picture where the ascii estimation of the content is changed over into a double worth and afterward it is installed into the lsb piece of the picture's pixels.

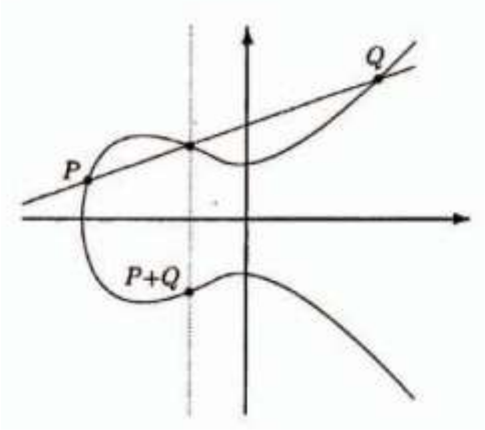
Image Encryption Utilizing Elliptic Curve Cryptography

A great many pictures are moved ordinarily across the organization. A portion of these pictures are private and we need these pictures to be moved safely. Cryptography assumes a critical part in moving pictures safely. The dramatically difficult issue to tackle an Elliptic Curve Discrete Logarithm Problem concerning key size of Elliptic Curve Cryptography, helps in furnishing an undeniable degree of safety with more modest key size contrasted with other cryptographic method which relies upon number factorization or Discrete Logarithmic issue. In this paper, we carry out the Elliptic Curve cryptography to encode, unscramble and carefully sign the code picture to give credibility and uprightness.

3.6. Point Addition

In Elliptic Curve Cryptography, activities are performed on the organize points of an elliptic bend. To perform expansion of two particular point facilitate the accompanying technique is utilized as demonstrated in the Figure 4.2. The point expansion is acted in the encryption part to encode the content.

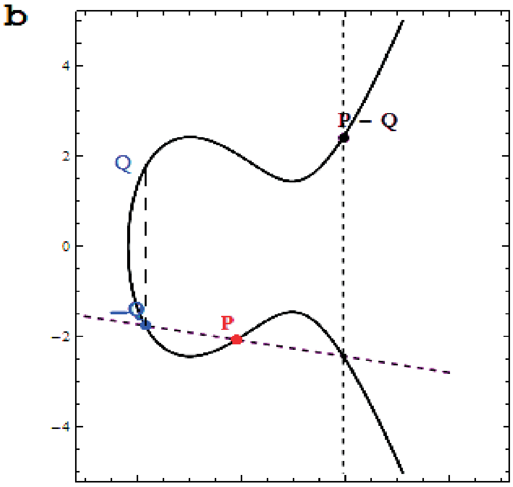
Figure 3- Point Addition



3.7. Point Subtraction

To perform point deduction, get a mirror arrange of the deducted point along x-pivot and perform point expansion on the subsequent organize and the other facilitate. The Figure 4.3 shows the point deduction work.

Figure 4- Point Subtraction



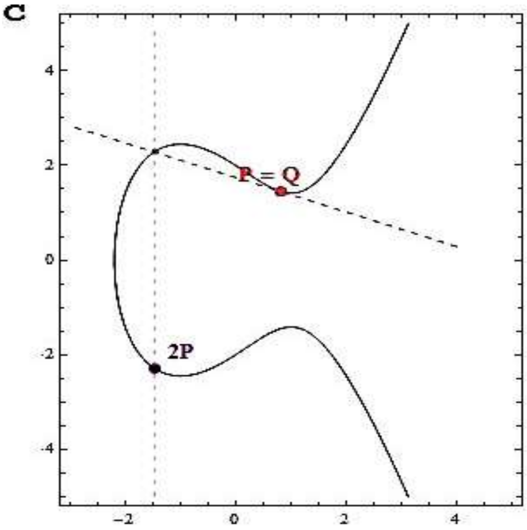
3.8. Point Doubling

Point multiplying is perform to include two focuses which are same for example they have same arrange esteem. Here point multiplying is acted in the key age measure for creating public and

Received: 03.03.2021 – Accepted: 08.04.2021

private key. The figure 4.4 is the point multiplying bend where it include two focuses which are same.

Figure 5- Point Doubling



De-Compression of the Picture is Performed

To begin with, 'Stego-Image' is taken and single exhibit of bytes are produced as it was done at the hour of encoding. The all out number of pieces of scrambled restricted data and the bytes addressing the 55 pixels of stego-picture are taken. Counter is at first set to 1, which thusly gives the record number of the pixel byte where mystery message digit is accessible in LSB. The cycle is proceeded till conclusive check of mystery message bit is reached. After this, the piece stream of the message will be produced. Accessible pieces are gathered to shape bytes with the end goal that every byte addresses single ASCII character. Characters are put away in text document which addresses the scrambled installed message. After that the unscrambling and decompression are to be performed.

4. Conclusion

The content encryption and decoding utilizing ECC holds great if the public key size isn't enormous. Besides the handling time will be more than the basic encryption strategy. Be that as it may, it is secure than the one layer of safety implemented by applying just encryption strategy for information. On the off chance that the privileged information is enormous, it must be compacted and other encryption technique ought to be utilized instead of ECC. For the situation it is needed to check the handling season of the strategy as it is the imperative boundary for the expense of preparing. In picture encryption and decoding utilizing ECC we have played out the activity by gathering the pixel. Matching of the gathered pixel esteem was performed as opposed to planning those qualities to elliptic bend facilitate. It assists with overlooking the utilized of reference planning table for encryption and decoding. Our calculation produces a low associated figure picture even with a picture which is comprised of same pixel esteem.

References

Shifa, A., Afgan, M.S., Asghar, M.N., Fleury, M., Memon, I., Abdullah, S., & Rasheed, N. (2018). Joint crypto-stego scheme for enhanced image protection with nearest-centroid clustering. *IEEE Access, 6,* 16189-16206.

Bhadra, J., Banga, M.K., & Murthy, M.V. (2017). Securing data using elliptic curve cryptography and least significant bit steganography. *In 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon),* 1460-1466.

Kim, C.R., Lee, S.H., Lee, J.H., & Park, J.I. (2018). Blind decoding of image steganography using entropy model. *Electronics Letters, 54*(10), 626-628.

Singh, L.D., & Singh, K.M. (2015). Image encryption using elliptic curve cryptography. *Procedia Computer Science Eleventh international multi-conference on information processing, 54,* 472-481.

Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S.W. (2016). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimedia Tools and Applications, 75*(22), 14867-14893.

Shetti, S., & Anuja, S. (2013). A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique. *International Journal of Engineering Research & Technology (IJERT),* Published by, ICESMART-2015 Conference Proceedings.

Ahmed, S.N., & Todwal, V. (2019). A Comparative Study of Image Steganography and Text Cryptography. *International journal of research in engineering, science and management, 2*(3), 820-823.

Ren-Er, Y., Zhiwei, Z., Shun, T., & Shilei, D. (2014). Image steganography combined with DES encryption pre-processing. *In Sixth International Conference on Measuring Technology and Mechatronics Automation,* 323-326.