An Improved LSB Image Steganography using Elliptic Curve Cryptography

M .Dinesh[a],P. Devaprasanth[b],M. Dhanasekar[c] ,Dr. N. S. Nithya [d],
a Student, Department of Computer Science and Engineering, K.S.R. College of Engineering, Anna University, Tiruchengode-637215, Tamilnadu, India murugandineshdk@gmail.com
b Student, Department of Computer Science and Engineering, K.S.R. College of Engineering, Anna University, Tiruchengode-637215, Tamilnadu, India mpdevaprasnth@gmail.com
c Student, Department of Computer Science and Engineering, K.S.R. College of Engineering, Anna University, Tiruchengode-637215, Tamilnadu, India dhanasekarmds423@gmail.com
d Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Anna University,Tiruchengode-637215, Tamilnadu, India sachinnithya2@gmail.com

ABSTRACT: Within the field of pc networks, cryptography and steganography are the well-known options for best security purpose. the most plan is to transmit the information firmly. So, providing acceptable level of security is crucial for knowledge transmission. conjointly it ought to cut back the time complexness of the protection algorithmic rule. Here we've used the "Elliptic Curve Cryptography" theme to code the information and image. A "Least important Bit" steganography algorithmic rule is employed to insert the encrypted knowledge to be hidden within the image so as to send the information firmly. The encrypted knowledge from the image is then decrypted by the coding algorithmic rule. Finally the hidden knowledge is taken from the decrypted knowledge. Then the image is compressed before causing through the net. MATLAB is employed to simulate results that show that it's smart embedding capability and security.

KEYWORDS: ECC, Data hiding, Information sharing, Data security, MATLAB

1 Introduction

Elliptic curve cryptography (ECC) is an approach to public-key cryptography technique based on the algebraic structure of elliptic curves over finite fields. Elliptic curve cryptography requires smaller keys when compared to non-Elliptic curve cryptography to provide equivalent security when compared to other algorithms and techniques. Elliptic curves are applicable for key generation, digital signatures, pseudo-random key generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a asymmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography method, such as Lenstra elliptic-curve factorization.

In computing, the least significant bit (LSB) is the bit position in a binary integer value giving the units value, that is, determining whether the number is even or odd. The Least significant bit is sometimes referred to as the lower-order or right most bit, due to the convention in positional denotation of writing less significant digits further to the right.

It is equivalent to the least significant digit of a decimal integer, which is the digit in the ones right most position. It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used here. Normally, this is simply the exponential of the corresponding bit weight in base. Although a few Control Processing Unit manufacturers assign bit numbers in the opposite way, the term least significant bit itself remains unidentified as an threat for the unit bit. By extension, the least significant bits are the bits of the number closest to, and including, the Least significant bit.

The easiest thanks to introduce secret data among the duvet image is termed the LSB insertion. during this technique, the binary representations of the key information are taken and therefore the LSB of every computer memory unit is overwritten among the image. If 24-bit color pictures area unit used, then the amount of modification are going to be little.

2 Block diagram

From the block diagram Figure 2.1, the message is being sent from the sender to the receiver. Then the message is hidden into the LSB of the image. This method is done by using the LSB steganography. Here, first the ASCII value of the text is known and then it is converted into the binary value. In the next step the text is embedded into the LSB of the image. The public key of the receiver is known to the sender. The original message is being encrypted using the receivers public key with the help of encryption algorithm. The encryption is done by using the Elliptic curve cryptography. The original message is then converted into the cipher text which is the encrypted message. The encrypted

© IJRAD.

message is then decrypted by using the receivers private key which matches the receivers public key. The decryption is then done by using the Elliptic curve cryptography. Thetext is then being taken from the LSB of the image.

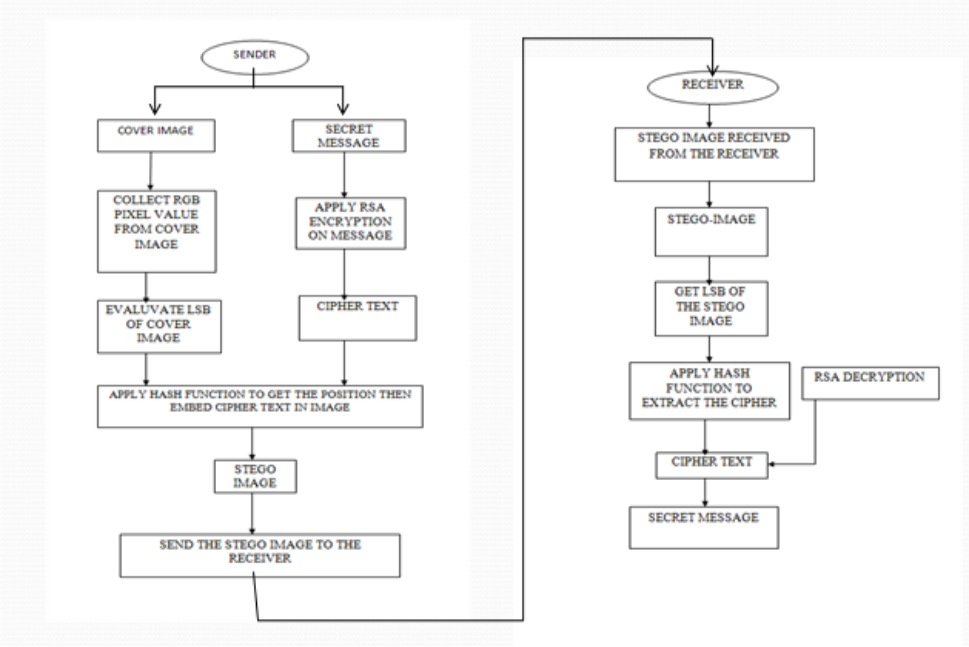

Figure 2.1 Block Diagram

3 Steganography

Steganography is that the technique of activity secret information among a standard, non-secret, file or message so as to avoid detection; the key information is then extracted at its destination. the employment of steganography will be combined with coding as an additional step for activity or protective information. The word steganography comes from the Greek words steganos (meaning hidden or covered) and therefore the Greek root graph (meaning to write).It will be wont to conceal virtually any kind of digital content, together with text, image, video or audio content; the info to be hidden will be hidden within virtually the other kind of digital content. The content to be hid through steganography known as hidden text is usually encrypted before being incorporated into the innocuous-seeming cowl computer file or information stream. If not encrypted, the hidden text is often processed in how so as to extend the issue of detective work the key content.

It is practiced by those wish to convey a secret message or code. whereas there area unit several legitimate uses for steganography, malware developers have conjointly been found to use steganography to obscure the transmission of malicious code. types of steganography are used for hundreds of years An embody nearly any technique for concealing a secret message in an otherwise harmless instrumentality. for instance, exploitation invisible ink to cover secret messages in otherwise inoffensive messages; concealing documents recorded on exposure which may be as little as one millimeter in diameter on or within legitimate-seeming correspondence; and even by exploitation multiplayer gambling environments to share data.

4 IMAGE ECC AND LSB-STEGANOGRAPHY

As that of the text encryption and decryption using elliptic curve cryptography the image is also encrypted using the encryption algorithm and decrypted using the decrypted algorithm in the receiver side

Image encryption using elliptic curve cryptography: legion pictures area unit transferred everyday across the network. a number of these pictures area unit confidential and that we need these pictures to be transferred firmly. Cryptography plays a big role in transferring pictures firmly. The exponentially exhausting downside to unravel Associate in Nursing Elliptic Curve separate log downside with relevance key size of Elliptic Curve Cryptography, helps in providing a high level of security with smaller key size compared to different science technique that depends on whole number factorization or separate exponent downside. during this paper, we tend to implement the Elliptic Curve cryptography to inscribe, decipher and digitally sign the cipher image to supply legitimacy and integrity.

A lot of knowledge is perceived after we observe a picture. pictures became associate inevitable supply of knowledge. each day we tend to stumble upon varied image from varied sources. once pictures area unit confidential and that we need the image to be transferred safe and firmly, cryptography comes into play. The cryptology technique that we've got enforced during this paper is that the Elliptic Curve Cryptography (ECC). varied study on computer code has terminated that the difficultly to resolve associate Elliptic Curve distinct index downside is exponentially laborious with relevancy the key size used. This property makes computer code a really good selection for encryption/decryption

© IJRAD.

method compared to different crypto logic techniques that area unit linearly tough or sub exponentially tough. computer code could be a public key cryptography that was developed by Neal Kollwitz and Victor S. Miller severally within the year 1985. computer code gains wide acceptance around 2004.

Point Addition: In Elliptic Curve Cryptography, operations are performed on the coordinate points of an elliptic curve. To perform addition of two distinct point coordinate the following method is used as shown in the Figure 4.1. The point addition is performed in the encryption part to encrypt the text.

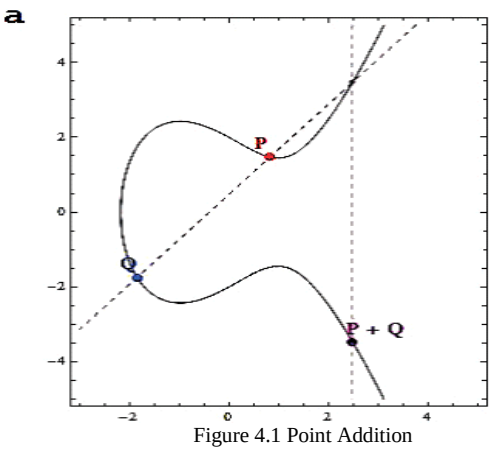

Figure 4.1 Point Addition

Point Subtraction: To perform point subtraction, get a mirror coordinate of the subtracted point along *x*-axis and perform point addition on the resulting coordinate and the other coordinate. The Figure 4.2 shows the point subtraction function.

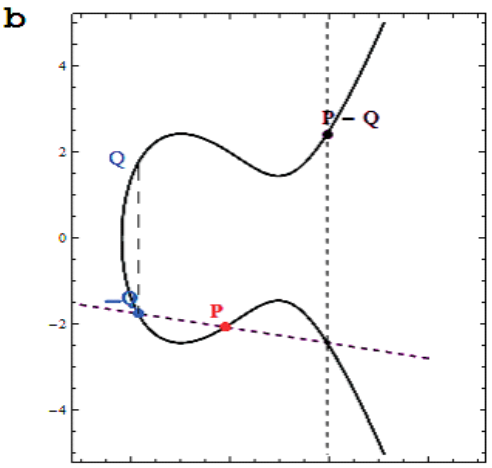

Figure 4.2 Point Subtraction

Point Doubling: Point doubling is perform to add up two points which are same i.e. they have same coordinate value. Here point doubling is performed in the key generation process for generating public and private key. The figure 4.3 is the point doubling curve where it add up two points which are same.

© IJRAD.

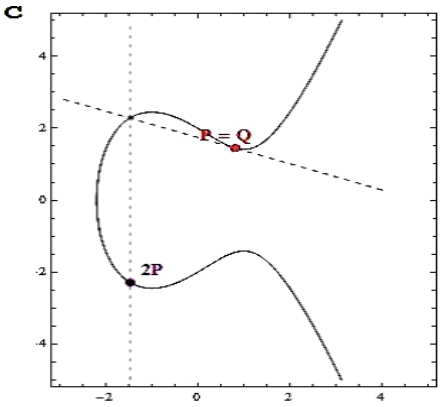

Figure 4.3 Point Doubling

Pixel grouping into one integer: pictures area unit created of pixels. If cryptanalytic operation is performed on each single picture element it'll take longer because the range of pixels gift is extremely massive. So, it'll be a decent choice to cluster the pixels along. the quantity of pixels to be cluster depends on the Elliptic Curve parameters used. The larger the parameter of the elliptic curve, the a lot of picture element is classified. as an example a 512 bit code parameter will cluster up to sixty three pixels along. to induce the quantity of pixels to be cluster, notice the quantity of the list, of the bottom 256 digits within the whole number ' p' minus one. To convert the cluster of pixels into an enormous single whole number we've used a perform of Mathematical referred to as From Digits [list of pixels, b] that take a listing of pixels and convert it to base b. we tend to add random one or a pair of to every picture element to avoid error caused whereas mistreatment From Digits perform of Mathematical, in case, the primary picture element price of the cluster is zero and additionally to produce low related to picture element price for the cipher image generated with same picture element price plain image. picture element price of image in computer memory unit kind can vary from zero to 255. therefore the most doable picture element price of the image are 257 {including as we tend toll as together with} the two we else. So, we'll use base price 'b' as 258.

Getting the cluster of pixels from the massive integer: once the ECC operation the coordinate worth can all be within the vary of the bit size chosen for the ECC operation. to get the cipher image from these coordinates we want to bring it all the way down to zero to 255 vary. we tend to performed mistreatment the number Digits [big number worth, 256] perform in Mathematic. It takes as input the massive number values within the vary of the scale chosen for ECC operation and with base 256, the output are an inventory of values starting from zero to 255. the 2 perform, From Digits [ ] and number Digits[ ] are inverse of every different that the pixels worth are preserved throughout the operation. operation on a picture is finished on the pixels worth of the image. So first, we tend to get the pixels worth of the image. The Elliptic curve parameters are in agreement between the sender and also the receiver. The sender use the general public key 'Pb' of the receiver to get the cipher image from the pixels of the plain image. The receiver use the non-public key 'n*B' that was accustomed generate the general public key, to decipher the cipher image back to the plain image. Here the component worth of the photographs are bought from the massive integers.

5 RESULT AND ANALYSIS

5.1 ENCRYPTION AND DECRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

Encryption and decryption of an image and the text is done by using the elliptic curve cryptography algorithm. This method is mainly done to transfer the image or a text in a secure manner.

5.1.1 Key generation and select the image

For data encryption and decryption, we should generate a public key, secret key and private key to transfer the data in a secure manner. The algorithms are given below.

5.1.1.1 User A key generation

- The sender A selects a random number kA from 1 to n-1.
- The sender A then generates the public key with the help of the formula
  public key P=kA*G
  kA - is the sender's private key
  G - Generation point

5.1.1.2 User B key generation

- The sender B generates the public key with the help of the formula
  public key R=kB*G
  kB - Receiver's private key
  G - Generation point

© IJRAD.

5.1.1.3 Secret key generation

- Secret key of A ,K=kA*R
  The secret key of A obtained by multiplying the private key A and the Public key of B.
- Secret key of B,K=kB*P
  The secret key of B is obtained by multiplying the private key of B and the key of A

5.1.2 Encrypt the data using the encryption algorithm

Encrypt the secret message with "elliptic Curve Cryptography" with the public key published by the receiver. The data is given in the text box as " kongu engineering college". This given data is encrypted in the sender side by using the encryption algorithm. Where we will use the public key for the encryption purpose.

5.1.2.1 Elliptic curve encryption algorithm

By using the encryption algorithm the text is encrypted by using the encryption algorithm

- The sender A needs to send a message 'pm' to the receiver B.
- Here the text pm is embedded with the help of taking the ASCII value of pm and multiplying it with a integer. The text now would be embedded in the point s.
- Here the cipher text Cm is obtained by using the formula
  Cm=(k*G, s + k*R) ,k - random integer, G - Generation point, pm - message
  R - public key of the receiver B
- The cipher text which is the encrypted text will be found in Cm which consists of a pair of points.

5.1.3 Decrypt the data from the image

Decrypt the data by using the private key in the receiver. Decrypt the text by using the decryption algorithm and retrieve the original text that is send by the sender.

5.1.3.1 Decryption algorithm

- To decrypt the cipher text the receiver B first multiplies the first point kG with the private key kB of the receiver B.

  $$kB(k*G)$$

- The receiver then subtracts the result from the second point

  $$Pm + k*R – kB(k*G)$$

- The receiver could then get the original text 'pm'.

5.1.4 STEGANOGRAPHY METHOD USING ELLIPTIC CURVE CRYPTOGRAPHY

The steganography method is used to hide the data inside the image at the least significant bit of the image's pixels. For the steganography method we have to choose a image to hide the data. The original image in which we have to hide the data in order to transfer the data in a more secure manner.

This method is used along with the elliptic curve cryptography which means the encrypted data is hidden inside the resized image. There will be no such difference between the resized image and the data hidden inside the image. The left side gives the resized image before the data is hidden. The right side image gives the encrypted data hidden inside the image.

5.1.5 IMAGE ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

Sometimes image cryptography mistreatment code are performed by mapping the picture element values to elliptic curve coordinate. For mapping, a separate hunt table is needed or used the purpose multiplication operation of picture element worth with generator 'G' to provide affine coordinate on the elliptic curve. In these cases, mapping table is needed whereas decipherment method to come up with the corresponding picture element worth from the cipher image. we tend to work on cluster of pixels to cut back the amount of computation. The cluster of pixels are reworked into massive whole number single digits keeping in mind that it shouldn't exceed 'p' worth that is one among the parameter in elliptic curve equation of finite field. These massive whole number values are paired and given as input denoted by 'Pm' in code operation. This operation facilitate North American nation to ignore the mapping operation and therefore the have to be compelled to share mapping table between sender and receiver.

5.1.4 Image encryption algorithm

The encrypted image from the original image using the encryption algorithm given below

© IJRAD.

- Get the pixel value of the image to be encrypted and arbitrarily add 1 or 2 to each pixel. Record the number of channels present in the image.
- Cluster the pixels and convert to single large integer value for each cluster. Number of pixel to be group using Mathematica is given by

  grp= Length [Integer Digits[p, 258]] – 1
- Pair up the result obtained from step 2 and store as 'Pm' which is the plain message input for the ECC system.
- Choose a random 'k' and compute 'kG' and 'kPb' where 'Pb' is the public key of the receiver.
- Perform point addition of 'kPb' with each value of 'Pm' and store as 'Pc' which is the cipher text.
- Convert the cipher text list from step 5 to worth starting value from 0 to 255.
- Pad left with 0 to each list from step 6 which have less than grp+ 1 number of elements, to create each list equal in length.

6 Software tool (MAT LAB)

MATLAB (matrix laboratory) may be a multi- paradigm numerical computing surroundings and proprietary programming language developed by Math Works. MATLAB permits matrix manipulations, plotting of functions and information, implementation of algorithms, creation of user interfaces, and interfacing with programs written in different languages, together with C, C++, C#, Java, algebraic language and Python. though MATLAB is meant primarily for numerical computing, associate degree ex gratia tool chest uses the MuPAD symbolic engine, permitting access to symbolic computing skills. an extra package, Simulink, adds graphical multi-domain simulation and model-based style for dynamic and embedded systems.

MATLAB has structure information varieties. Since all variables in MATLAB are arrays, a lot of adequate name is "structure array", wherever every part of the array has identical field names. additionally, MATLAB supports dynamic field names (field look-ups by name, field manipulations, etc.). sadly, MATLAB JIT doesn't support MATLAB structures, thus simply an easy bundling of varied variables into a structure can return at a value.

When making a MATLAB perform, the name of the file ought to match the name of the primary perform within the file. Valid perform names begin with associate degree grapheme, and might contain letters, numbers, or underscores. Functions area unit typically case sensitive. MATLAB supports components of lambda calculus by introducing perform handles, or perform references, that area unit enforced either in .m files or anonymous nested functions.

MATLAB includes GUIDE (GUI development environment) for diagrammatically planning GUIs. It conjointly has tightly integrated graph-plotting options. for instance, the perform plot is accustomed turn out a graph from 2 vectors x and y.

MATLAB will decision functions and subroutines written within the programming languages C or FORTRON. A wrapper operate is formed permitting MATLAB information varieties to be passed and came back. The dynamically loadable object files created by collecting such functions. Since 2014 increasing two-way interfacing with python was being additional. Libraries additionally exist to import and export.

Libraries written in Perl, java, or .NET will be directly known as from MATLAB, and lots of MATLAB libraries are enforced as wrappers around Java or ActiveX libraries. line MATLAB from Java is a lot of difficult, however will be finished a MATLAB tool case that is sold-out on an individual basis by maths works, or victimization associate unsupported mechanism known as JMI (Java-to-MATLAB Interface), that shouldn't be confused with the unrelated java information bury face that's conjointly known as JMI. Official MATLAB API for Java was further.

MATLAB could be a proprietary product of mathematics Works, thus users area unit subject to vendor-lock in .Although MATLAB Builder merchandise will deploy MATLAB functions as library files which might be used with .NET or JAVA application building atmosphere, future development can still be tied to the MATLAB language. every tool case is purchased singly. If associate degree analysis license is requested, the maths Works sales force needs elaborate info regarding the project that MATLAB is to be evaluated.

7 CONCLUSION

The text secret writing and decoding victimization error correction code holds sensible if the general public key size isn't terribly giant. Furthermore the intervals are going to be quite the easy secret writing technique. However it's secured than the one layer of security enforced by applying solely secret writing technique of information. If the key information is giant then it's to be compressed and different secret writing technique ought to be utilized in place of error correction code. Within the case it's needed to see the interval of the tactic because it is that the very important parameter for the price of process. In image secret writing and decoding victimization error correction code we've got performed the operation by grouping the component. Pairing of the sorted component worth was performed rather than mapping those values to elliptic curve coordinate. It helps to ignore the used of reference mapping table for secret writing and decoding. Our rule generates a coffee correlate cipher image even with a image that is formed of same component worth.

© IJRAD.

References

[1] Amna Shifa, Muhammad Sher Afgan, and Muhammad Sher Afgan (2018), "Joint Crypto-Stego Scheme for Enhanced Image Protection with Nearest-Centroid Clustering"

[2] Jayati Bhadra, Banga.M.K, Vinayaka Murthy (2018), " securing data using elliptic curve cryptography and least significant bit steganography", International conference on smart technology for smart nation, IEEE Explore, volume 86.

[3] Kim.C.R, Lee S.H, Lee.J.H, Park.J.I (2018) "Blind decoding of image Steganography using entropy model", electronics letters IEEE Explorevolume:54,issues:10.

[4] LaiphrakpamDolendro Singh and KhumanthemManglem Singh (2015)," Image encryption using elliptic curve cryptography", eleventh international multi-conference on information processing, vol 54, pp 472-481.

[5] Muhammad.K (Nov 2016), "A Novel Magic LSB Substitution Method (M-LSB-SM) using multi-level encryption and achromatic component of an image", Springer Link, volume 75, issue 22, pp 14867-14893.

[6] Ms.ShrideviShetti and Mrs.Anuja S (2013), "A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, ICESMART-2015 Conference Proceedings, issue 2015.

[7] Shabina N. Ahmed and Vinod Todwal (2019)," A Comparative Study of Image Steganography and Text Cryptography", International journal of research in engineering, science and management, volume 2, issue 3.

[8] Yang Ren-Er , Zheng Zhiwei ; Tao Shun ; Ding Shilei (2014) , "Image Steganography Combined with DES Encryption Pre-processing", 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, volume 03, issue 54.

© IJRAD.