Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography

Ravneet Kaur
Computer Science & Engineering Department
ACET Amritsar, India

ABSTRACT
Multimedia data security is becoming important with the continuous increase of digital communication on the internet. Without having privacy of data there is no meaning of doing communication using extremely high end technologies. Data encryption is suitable method to protect data, where as steganography is the process of hiding secret information inside some carrier. This paper focus on utilization of digital video/images as a cover to hide data and for insinuating more security encryption is done with steganography. In the proposed method encrypting message image with ECC and hiding encrypted image using LSB within cover video. It gives a high level of authentication, security and resistance against extraction by attacker. As ECC offer better security with smaller key sizes, results in faster computation , lower power consumption as well as memory and bandwidth saving.

Keywords
Cover Video, Steganography Elliptic curve cryptography (ECC),PSNR(Peak signal to noise ratio), MSE (Mean square error)

1. INTRODUCTION
In the field of Data communication top priority of 21th century is Security. With the development of network technologies and coming of digital era, computers and use of internet becomes a part of life. So securing the information becomes an issue. The concept of hidden exchange of information is concerned. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher and hide their existence. Steganography is the science of hiding messages in a medium called carrier or cover in such a way that existence of the message is concealed. The cryptography is also used to provide security to data over network, by converting plain text into cipher text. Cryptography makes necessary elements for secure communication namely privacy, confidentiality, key exchange and authentication but reveals the fact that communication is happening. Steganography takes cryptography a step farther by hiding the existence of the information. Steganography methods can be classified into spatial domain embedding and frequency domain embedding. Least Significant Bit(LSB) replacing is the most widely used steganographic method in spatial domain,which replaces the cover image’s LSBs with message bits directly. LSB is popular because of its low computational complexity and high embedding capacity.[1] Different types of algorithms in cryptography and steganography so that the hackers cannot identify which algorithms is supposed to be used.In Public cryptography we have Elliptic curve cryptography(ECC),Digital Signature algorithm (DSA) , Diffie-Hellman and RSA algorithms are mostly used. Both steganography and cryptography are data security techniques. Steganography can use cryptography where as cryptography cannot use steganography. Steganography implemented to cryptographic data will increase in security level.

Elliptic Curve cryptography (ECC) is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. With smaller key sizes and lower processing requirements than other public key cryptosystems, elliptic curve cryptography lends itself well to sending information securely over the internet where bandwidth and processing capabilities are limited. Ensuring the timely and reliable access to make use of information.ECC offers security with smaller key sizes, faster computation, lower power consumption as well as memory and bandwidth saving .This is especially useful for mobile devices,wireless pagers which are limited in bandwidth,memory and low Power and network connectivity.[2] The mobile apps such as multimedia messages, whatsapp are new standards in mobiles era used for communication.

Elliptic curve cryptography is an asymmetric key cryptography. It includes public key, private key and set of operations associated with the keys to do cryptographic operations. Public key may be freely distributed where as private key is kept secret. the public key is used for Encryption , while the private or secret key is used for decryption. Some public key algorithms may require a set of predefined constants to be known by all the users taking part in communication. Domain parameters in ECC is an example of such constants.[4] The choice of the type of elliptic curve is dependent on its domain parameters, the finite field representation, elliptic curve algorithms for field arithmetic as well as elliptic curve arithmetic[3]

An elliptic curve in its “standard form” is described by
\[ y^2 = x^3 + ax + b \]  
(1)

For the polynomial \( x^3 + ax + b \), the discriminant can be given as
\[ D = -4a^3 + 27b^2 \]  
(2)
\[ 4a^3 + 27b^2 \neq 0 \]

This discriminant must not become zero for an elliptic curve polynomial \( x^3 + ax + b \) to possess three distinct roots. If the discriminant is zero, that would imply that two or more roots have coalesced, giving the curves in singular form. It is not safe to use singular curves for cryptography as they are easy to crack. Each value of a and b gives different elliptic curve. All points (x,y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. An elliptic curve cryptosystem can be defined by picking a prime number as a maximum, a curve equation and a public point on the curve.A private key is a random number, public key is obtained by multiply the private key with the generator point G in the curve.

Tanupreet Singh, Ph.D
Electronic and Communication Engineering Dept
ACET, Amritsar, India
An elliptic curve over a prime field is defined as follows,
\[ y^2 \mod p = (x^3 + ax + b) \mod p \]
p is a prime number

This paper is organized as follow, Section II will give about the basic model of proposed work. Section III defines methodology of proposed work. Section IV will cover parameters, Section V will consist of results and discussions. Section VI describes conclusion.

2. BASIC MODEL
The model of proposed algorithm (Fig :1) uses cover video as a carrier for secret data ,input secret file is the data that is to be sent secretly. Encryption technique is used to convert secret data into encrypted file for more security of data. Embedding Technique is the procedure to hide encrypted message in cover video and results in stego video. Stego video contains the secret data. Stego video transmits through communication channel . Receiver will get encrypted data from stego video by extraction technique but get the original data after decryption of secret file.

3. PROPOSED WORK
Our work is classified into two parts.

3.1 Cryptography

Before hiding message image inside video, Encrypt image with ECC.

This algorithm first converts an image into binary and then map, A square grid of required size is constructed by taking the binary data from source file. As the image is now seen as a grid, every pixel of this is first mapped on the elliptic curve by applying the gen point (a, b, p).

Next the pixels are encrypted using ECC.

Then hide encrypted image in video using steganography.

3.2 Video/Image Steganography
A video consist of set of frames (digital images) that are played back at certain frame rates based on video standards. The size of image is m*n ,it is composed of m pixels in horizontal direction(rows) and n pixel in vertical direction(columns). RGB color image has three frames of image. 24 bits are required to represent a pixel of color image. LSB method is used to hide data in images/videos. To hide a message image divide video into M frames. Each Selected frame will have histograms. Appropriate pixels are determined by comparing histograms of the frame. Each pixel in each frame has LSB. Hide each bit of encrypted message into LSB of pixel. Select pixel for hiding data using password which will be shared by sender and receiver.

4. PARAMETERS USED
We demonstrate the performance of our purposed method.

The parameters used in this paper are:

PSNR------The image/video quality of each steganography method is expressed in PSNR (Peak Signal to Noise ratio). PSNR measure the quality of the video by comparing original video with stego video The higher the PSNR, the better the quality of the compressed or reconstructed image. The PSNR values can be obtained using following formula:

\[ \text{PSNR}=10 \log_{10} \left( \frac{\text{MAX}^2}{\text{MSE}} \right) \]

MSE--------Mean square Error is the measure used to quantify the alteration between the initial and the distorted video. MSE is calculated with the following formula.

\[ \text{MSE} = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (C(x,y)-S(x,y))^2 \]

Embedding capacity------It represents the embedded secret bits in the cover image. According to payload evaluation embedding capacity represents that steganographic scheme has better performance in terms of embedding payload that is pixels in cover image can carry more secret bits. How ever
the embedding capacity of our proposed algorithm is 230400 and it seems to be good.

5. RESULTS AND EVALUATIONS

In this section we report the implementational results. we use “xylophone.mpg” as a cover video and “cat.jpg” as the message image to hide under MATLAB software. Later we implement the algorithm on different images as shown in table the MSE and PSNR are parameters used to measure alteration and distortion between original and stego video. Experimental results show that proposed algorithm improves the embedding capacity, maintains quality of stego video as well as provide security to secret message.

6. OBTAINED RESULTS

Fig 2: Cover video

Fig 3: Hidden image

Fig 4: PSNR Graph

Fig 5: MSE graph
The value of PSNR results above 52db as an average for different images which shows that quality of stego video is best. As a high quality stego–video struggle for 40db.

Improved PSNR shows that quality of image and stego video also have higher level of security.

As M.S.E has zero as an average value that sure’s that received image remains same as original sending image. As there is minor bit error rate represented by BER Graph, but the overall difference between pixels remain negligible.

7. CONCLUSION

This paper introduces the concept of combination of steganography and elliptic curve cryptography. The attractiveness of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. As per the results obtained steganography when combined with cryptography provides higher levels of security. The cover image is protected with personal key(password)so it is not possible to damage data by unauthorized person. The resolution does not affected much and is negligible. Hece this paper focuses on increasing security, increasing PSNR and reducing distortion rate.

The encryption using ECC is new domain and has tremendous scope of research.

8. REFERENCES


Elliptic curve cryptography, an implementation guide, Anoop MS


Unik Lokhande,”An Effective Way of using LSB Steganography in images along with Cryptography” International Journal of Computer Applications (0975 – 8887) Volume 88 – No.12, February 2014


