Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography

Ravneet Kaur
Computer Science & Engineering Department
ACET Amritsar,
PTU Jalandhar,India

Tanupreet Singh, Ph.D
Electronic and Communication Engineering Dept
ACET,Amritsar
PTU Jalandhar,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 insisting 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 band width 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

$$y2 = x3 + ax + b \quad \ldots\ldots(1)$$

For the polynomial $x3 + ax + b$, the discriminant can be given as

$$D = - (4a3 + 27b2) \quad \ldots\ldots(2)$$

$$4a3+27b2 \neq 0$$

This discriminant must not become zero for an elliptic curve polynomial $x3 + ax + b$ 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.

An elliptic curve over a prime field is defined as follows,

y2 mod p=(x3 + ax + b)mod p ,p is a prime number

This paper is organized as follow, **Section II** will give about the basic model of purposed 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 compairing 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.

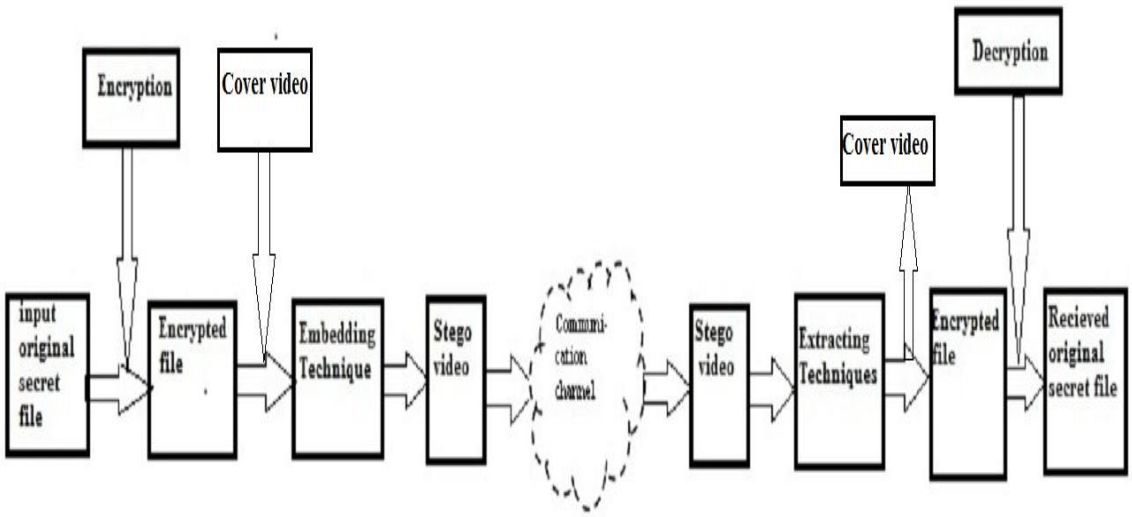

Fig:1 Basic Model

This method provides double security, if unauthorized person some way extract the message image from video . He will not read the message because it is encrypted with senders private key using ECC.

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:

$$\mathbf{PSNR=10log_{10}(MAX^2/MSE)}$$

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.

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

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.

Fig 2: Cover video

6. OBTAINED RESULTS

Fig 3:Hidden image

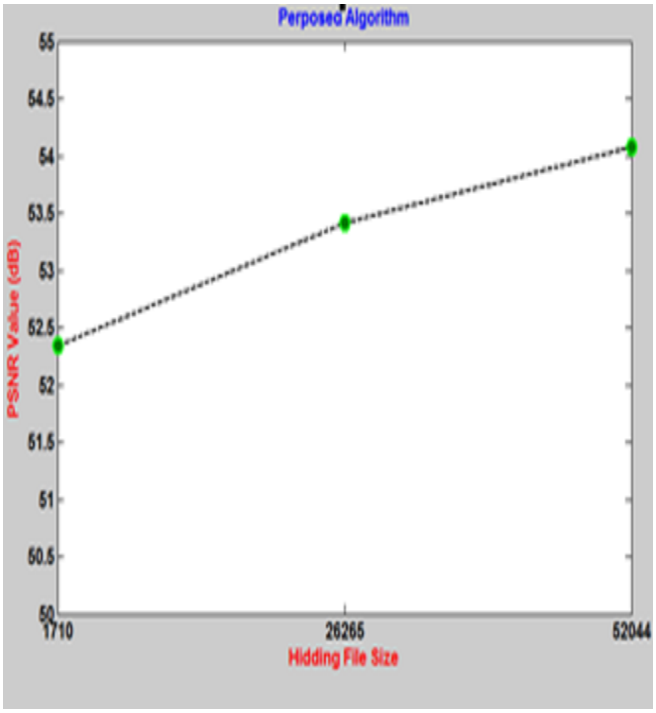

Fig4: PSNR Graph

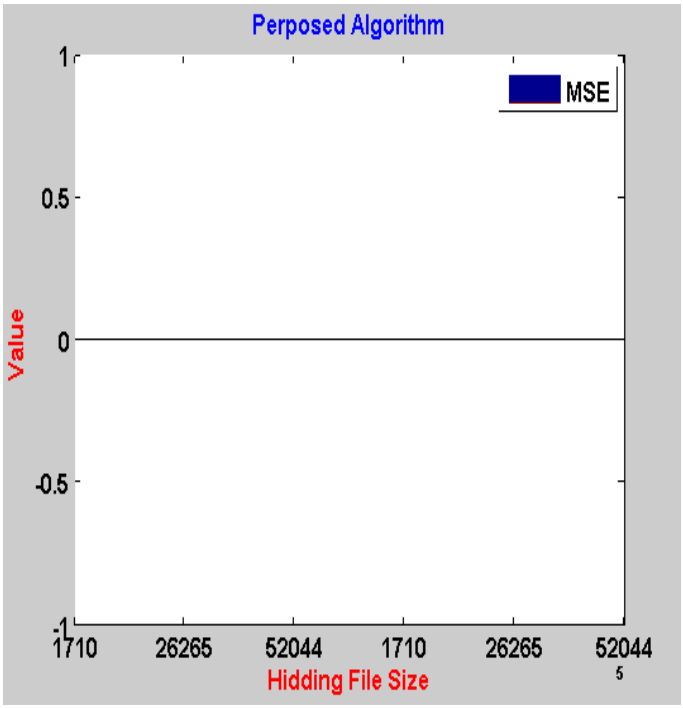

Fig 5: MSE graph

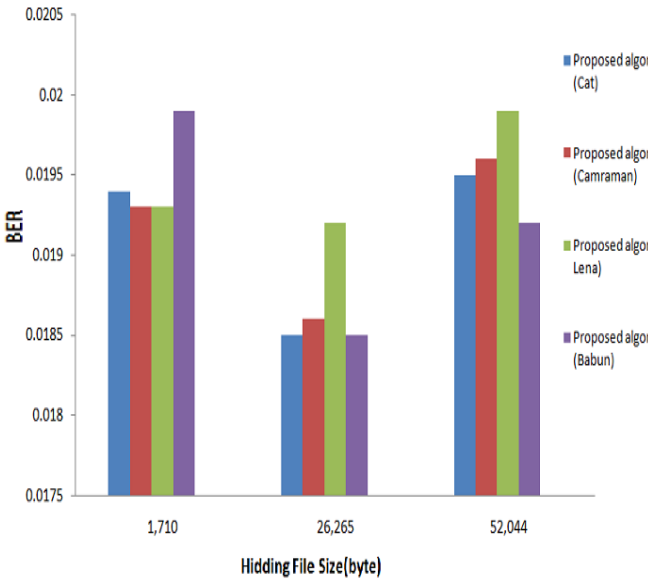

Fig 6:BER Graph

a b c d

Hiding File size	Proposed algorithm			
Hiding file size(byte)	PSNR (a)	PSNR (b)	PSNR (c)	PSNR (d)
1,710	52.34	50.79	51.6157	53.6913
26,265	53.41	54.61	52.37	53.1
52,044	54.08	54.34	52.58	51.9

Table: 1.1 PSNR values of Proposed Algorithm

From the results it can be concluded that the embedding capacity in algorithm is good. As the proposed algorithm has embedded capacity=230400.

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 demage 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

[1] Lifang Yu,Yao Zhao,"Improved Adaptive LSB Steganography Based on Chaos and Genetic algorithm",EURASIP Journal on Advances in Signal Processing 2010,2010:876946 doi:10.1155/2010/876946

[2] Samta Gajbhiye ,Dr. sanjeev Karmakar"Application of Elliptic curve Method in cryptography:A Literature Review", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4499 – 4503

[3] Tarun Narayan Shankar, G.Sahoo," Cryptography by Karatsuba Multiplier with ASCII Codes" ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12

[4] B.N Jagdale ,R.K Bedi"Securing MMS with high performance Elliptic curve cryptography",International journal of computer applications (0975-8887)volume 8-No.7,October 2010

[5] Dr. ParmaNand Astya, Ms. Bhairvee Singh," IMAGE ENCRYPTION AND DECRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY" IJARSE, Vol. No.3, Issue No.10, October 2014 ISSN-2319-8354(E)

[6] S. Maria Celestin Vigila , K. Muneeswaran," Implementation of Text based Cryptosystem using Elliptic Curve Cryptography". 978-1-4244-4787-9/09/$25.00 ©2009 IEEE

[7] Hailiza Kamarulhaili and Liew Khang Jie," Elliptic Curve Cryptography and Point Counting Algorithms" www.intechopen.com

[8] Shery Elizabeth Thomas, Sumod Tom Philip**,"** Advanced Cryptographic Steganography Using Multimedia Files", International Conference on **Electrical Engineering and Computer Science**

(ICEECS-2012), May 12th, 2012, Trivendum, ISBN Number : 978-93-81693-58-2

[9] Elliptic curve cryptography,an implementation Guide,Anoop MS

[10] Rosziati Ibrahim and Teoh Suk Kuan," Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

[11] C Abikoye Oluwakemi "Efficient Data Hiding System using Cryptography and Steganography "International Journal of Applied Information Systems (IJAIS) ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4 – No.11, December 2012 – www.ijais.org

[12] **Jolly shah and Dr. Vikas Saxena,"** Video Encryption: A Survey", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814,www.IJCSI.org

[13] Saraswati Singh, Nilmani Verma," A Survey Report on Video Encryption and Decryption Techniques" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014, pg. 270-274.

[14] 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

[15] Shamim Ahmed Laskar1 and Kattamanchi Hemachandran," High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012

[16] Sujay, N. and Gaurav, P.2010. "Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions". *Signal & Image Processing: An International Journal (SIPIJ)*, 1(2), pp 60-73.

[17] [17] Pranab Garg ,Jaswinder singh Dilawari"A Review paper on cryptography and significance of key lengh" International journal of computer science and communication Engineering. IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012

[18] Li, S., Chen, G., Zheng, X.: Multimedia security handbook. Internet and Communications Series, vol. 4, chap. Chaos-Based Encryption for Digital Images and Videos, pp. 133–167. CRC Press, West Palm Beach (2004)

[19] C.-K.Chan and L.-M. Cheng,"Hiding data in images by simple lsb substitution," Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.

[20] Y. Zhang, F. Zuo, Z. Zhai, and C. Xiao bin, "A new image encryption algorithm based on multiple chaos system," in Proceedings of the International Symposium on Electronic Commerce and Security (ISECS '08), pp. 347–350, August 2008.

[21] O.CETIIN and A.OZCERIT, "A new Steganography Algorithm Based on Color Histograms for Data Embedding into Raw Video Streams", Elsevier Ltd ,Computers & Security, Sakarya University, Turkey,Vol.28, pp. 670-682 , 2009.

[22] S. Suma Christal Mary, "Improved Protection in Video Steganopgraphy Used Compressed Video Bit stream," International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397

[23] A. Vashistha, R. Nallusamy, A. Das, S. Paul, "Watermarking video content using visual cryptography and scene averaged image", 2010 IEEE International Conference on Multimedia and Expo, pg. 1641-1646, September 2010

[24] J. Shah, V. Saxena, "Video Encryption: A Survey" International Journal of Computer Science Issues, Vol. 8, No. 2, pg. 525-534, March 2011

[25] M. Abomhara,, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.

[26] Vismita Nagrale, Ganesh Zambre and Aamir Agwani, "Image Stegano-Cryptography Based on LSB Insertion & Symmetric Key Encryption", International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 2, Issue 1, 2011, pp. 35 - 42, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.

[27] Sharma V.K., Shrivastava V.,"A steganography algorithm for hiding image in image by improved LBS substitution by minimize detection", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 1,pp. 1-8, 2012.