ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

Enhanced Database Security using ECC, Steganography and Watermarking.

Shilpashree s. Student Dept of ECE DBIT, Bengaluru
SOWMYA K S, Associate Professor DBIT ,Bengaluru.

Abstract— ***Abstract- Data encryption and authentication is important to protect data and ensure the security over internet. A new method has been proposed in this paper by combining Elliptic curve cryptography (ECC), Steganography and Watermarking techniques to provide data encryption and higher level of security to confidential data with lesser key size. Each plaintext of database is converted into hexadecimal ASCII value of two digits, then value is divided into two values. After that each value transformation is performed into an affine point on the elliptic curve. This transformation is used to encrypt/decrypt the message. Steganography is applied on the encrypted data using double stegging into cover image, then the host image is watermarked on cover image using SVD watermarking for authentication. By using this method the number of doubling operations can be reduced and whole data can be stored in the same memory.***

Index Terms : *Data encryption, Elliptic curve cryptography, Double stegging, SVD watermarking*.

1. INTRODUCTION

Internet is responsible for the communication between millions of people around the world and it is increasingly used a tool for many organizations hence data security is very crucial.

Cryptography is the science that enables secure communication in the presence of malicious adversaries by encrypting data into cipher text (encrypted text). The text is decrypted only by those who possess a secret key. Two main categories of cryptography are symmetric key cryptography and public key cryptography. In symmetric key cryptography same key is used for encryption and decryptions on the other hand in public key cryptography different keys are used for encryption and decryption.

1n 1985 koblitz and miller independently proposed the implementation of public key cryptosystem using elliptic curve over finite field which is called elliptic curve cryptography (ECC). ECC each device or user taking part in the communication will be having number of keys that is private key and public key and number of operations associated with those Public key is shared with all the users and particular users have their own private key. Public key algorithm uses "domain parameters" which are Constants for cryptographic operations.

Steganography is art of hiding the secret data into cover image by concealing its existence which is used for transmission and communication. Steganography can utilize various medium as carriers of the message. These mediums may include the classical methods of steganography using text, like character marking, invisible ink, using pin pictures, type-writer correction), images, and audio, video signals . In this paper steganography is applied for two times to embed encrypted data into the area of sharp region hence the name double stegging.

Digital Watermark is piece of digital information that may image or code which is embedded in the in the digital content in such a way that it is inseparable from its data. This piece of information known as watermark, a tag, or label into multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video, or text. SVD (singular value division) based watermarking is used in this paper to provide watermark with minimal distortion. Output of this watermark is more secure and robust.

II. RELATED WORK

Many Authors works on ECC, double stegging and watermarking strength and implementation. [1]Victor s Miller, explain about the elliptic curves in cryptography, his encryption scheme is similar to Diffie hellman key exchange but faster than that. [2]Neal Koblitz, explains that security of ECC depends on ECDLP complexity and also explains ECDLP is harder for finite group field compared to binary field. [5]Debrath Boruah, Monjul saikail, explains about the elgamal elliptic curve cryptosystem and is implementation using c language in their work. Different algorithms are also used in the implementation to perform various mathematical manipulations. [7]Arun kumar ray,sabya sachi padihery,prashant kumar patra explains about new watermarking algorithm based on SVD. They encrypt and embed the singular values of watermark instead of original singular values. PSNR ratio is used to measure the imperceptibility.[8] Kotagiri Ramu , Kalpana Reddy paper focused on identifying the sharp regions and using them adaptively of data hiding. Double stegging method has been compared with other methods such as PVD method, LSB matching method.[9] [10] Maria Celestin and K. Muneeswaran used decimal ASCII value to represent the

characters. These characters are transformed into points on the elliptic curve through multiplying their values by a random point on the Elliptic Curve9

III. PROPOSED WORK & EXECUTION

This paper increases the security strength of the confidential data to higher level by combining the techniques of ECC, Steganography and Watermarking

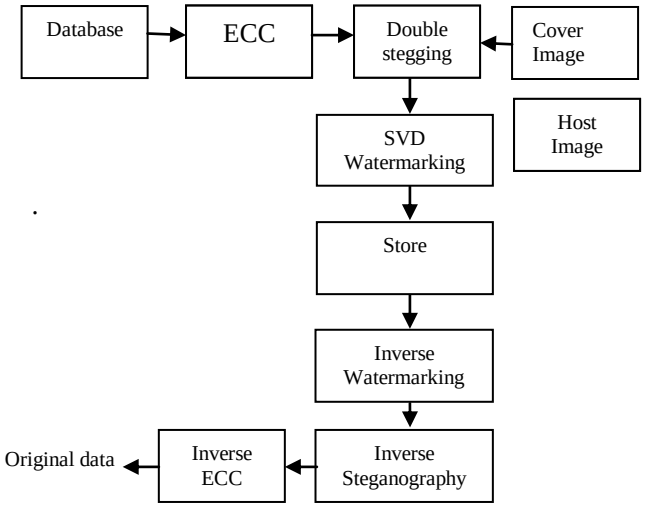

Fig 1. The overall system design block diagram.

[1] ECC

The confidential data that registered in the first part is encrypted using ECC. Equation of the elliptic curve on a prime field F_p is

$$y^2 mod p = x^3 + ax + b mod p \quad (1)$$

Where $a, b \in F_p$ and satisfy the condition $4a^2 + 27b^2 \neq 0 (mod p)$. The set of all points (x, y) that satisfy an elliptic curve equation (1), with a special point o(point at infinity), forms an elliptic curve group $E(F_p)$. Elliptic curve crypto system first converts the plaintext 'm' into point p_m on the elliptic curve $E(F_p)$. The domain parameters (a, b, G, p) of elliptic curve are public for all devices/users in communication. If S and R are two users wishes to exchange the information over internet. S and R needs to choose their private key. The private keys, n_s and n_r are positive integers that range between 1 to p-1.

The public key of S and R is generated using the relation,

$$P_S = n_s . G \quad (2)$$

$$P_r = n_r . G \quad (3)$$

Each character in message is converted into hexadecimal ASCII $(h_1 h_2)_{16}$ then it is separated into value of h_1, h_2 to decimal values d_1 and d_2, these values are transformed to point on elliptic curve using the relation,

$$P_{d1} = d_1 . G \quad (4)$$

$$P_{d2} = d_2 . G \quad (5)$$

P_{d1} And P_{d2} are two points lies on elliptic curve.

Sender S computes the secret key K using the relation.

$$K = n_s . P_r \quad (6)$$

To compute cipher text, value of K, P_{d1}, P_{d2} values are used

$$C_1 = P_{d1} + K \quad (7)$$

$$C_2 = P_{d2} + K \quad (8)$$

C_1 and C_2 are two points lies on elliptic curve.

Upon receiving the cipher text C_1 and C_2 by receiver R, the decryption process started. Receiver R gets the secret key using the relation,

$$K = n_r . P_s \quad (9)$$

then subtracts K from C_1 and C_2 to get P_{d1} and P_{d2}.

$$C_1 - K = C_1 - n_r . P_s \quad (10)$$

$$= P_{d1} + n_s . P_r - n_s . n_r . G$$

$$= P_{d1} + n_s . n_r . G - n_s . n_r . G$$

$= P_{d1}$ and in similar way for C_2

Next step is to solve the equations for d_1 and d_2 by using elliptic curve discrete logarithm problem where P_{d1} and P_{d2} and G are known. The last step is to convert d_1 and d_2 to h_1, h_2 then find the match character from hexadecimal ASCII table. And the previous procedure is repeated for each message m.

The advantage of using this method is solution for P_{d1} and P_{d2} for the receiver is easy and will not take long time because largest value for d_1 and d_2 in decimal is 15. But it is very difficult for the adversary because he cannot know the private key n_r and prime number p will be chosen as large number.

Implementation example:

Assume the user "S" and user "R" are agreed to use the elliptic curve

$$y^2 mod p = x^3 + ax + b mod p$$

Where $a = 1$ and $b = 3$ and $p = 31$ satisfy the condition $4a^2 + 27b^2 \neq 0 (mod p)$=$4(1^3) + 27(3^2) = 247 mod 31$ =30≠0, then points on the elliptic curve are shown in table 1

Table 1. points on the elliptic curve

(1,6)	(1,25)	(3,8)	(3,23)	(4,3)	(4,28)	(5,3)	(5,28)
(6,15)	(6,16)	(9,11)	(9,20)	(12,10)	(12,21)	(14,8)	(14,23)
(15,13)	(15,18)	(17,2)	(17,29)	(18,5)	(18,26)	(20,5)	(20,26)
(21,4)	(21,27)	(22,3)	(22,28)	(23,14)	(23,17)	(24,5)	(24,26)
(26,11)	(26,20)	(27,11)	(27,20)	(28,2)	(28,29)	(30,1)	(30,30)

Let the point (1,6) is chosen as base point G ,and selected domain parameters are (a, b, G, p)=(1,3,{1,6},31) ,when

sender wants to send message to receiver ,sender should first convert each character in message to hexadecimal value of ASCII table, then separates each value into two values and converts them to decimal values.

S→$(53)_{16}$→$(5,3)_{16}$→$(5,3)_{10}$
t→$(74)_{16}$→$(7,4)_{16}$→$(7,4)_{10}$
u→$(75)_{16}$→$(7,5)_{16}$→$(7,5)_{10}$
d→$(64)_{16}$→$(6,4)_{16}$→$(6,4)_{10}$
e→$(65)_{16}$→$(6,5)_{16}$→$(6,5)_{10}$
t→$(74)_{16}$→$(7,4)_{16}$→$(7,4)_{10}$

Proposed algorithm is applied to each character, first each character is converted into hexadecimal value from ASCII table, and obtained value is separated into values and converts it to decimal value, then do following calculation.

Key scheduling:

User "S"

- Choose private key n_s=13€(1 ,30)
- Compute public key P_S=n_s. G =13(1,6)=(3,23)

User "R"

- Choose private key n_r=17€(1 ,30)
- Compute public key $P_r = n_r . G$= 17(1,6)=(24,5)

P_S and P_r will be exchanged and public for both "S" and "R"

Encryption:

User "S"

- S→$(53)_{16}$
- $P_{d1} = d_1 . G$ =5(1,6)=(15,18)
- $P_{d2} = d_2 . G$ =3(1,6) =(12,10)
- $K = n_s . P_r$ =13(24,5)=(20,5)
- C_1=P_{d1}+ K =(15,18)+(20,5)=(4,3)
- C_2=P_{d2}+ K= (12,10)+(20,5)=(27,11)

Send (15,5) , (9,14) to user S

Decryption:

- $K = n_r . P_s$=17(3,23)=(20.5)
- P_{d1}=C_1-k=(15,5)-(20,5)=(15,18)
- P_{d2}=C_2-k=(9,14-(20,5))-=(12,10)
- Extract d_1 =5 from P_{d1} by solving discrete logarithm problem (15,18)= d_1 (1,6)
- Extract d_2 =3 from P_{d2} by solving discrete logarithm problem (12,10)= d_2(1,6)
- Convert $(5,3)_{10}$ to hexadecimal $(5,3)_{16}$ and rewrite it as $(53)_{16}$.
- Find the match character for $(53)_{16}$ from hexadecimal ASCII table which is "S"

The same process for other characters "udent" should be repeated.

[2] Steganography

The goal of the steganography is to embed confidential data into cover image in such a way that its existence is concealed. The DWT of the cover image is obtained by analysis filter pair, resulting two dimensional coefficients contains four bands of data .each labeled as LL (low-low), LH (low-high), and HL (high- low), LH (low-high) and (high-high).

DWT provides one approximation and three detail coefficients on each decomposition level. An approximation coefficient contains the most information content hence detail coefficients are used for message hiding.

The encrypted details C_1 and C_2 from ECC encryption is embedded to the cover image for two times hence the name double stegging. First data is embedded to HH region and multiplying with some constant values, data is transferred is transferred to HL region. Double stegging increases the security strength of original data.

[3] SVD Watermarking.

Singular value decomposition watermarking is used in this paper. The host image is first decomposed into sub-bands by applying DWT. The watermark image is embedded in all the sub-bands by modifying singular values of each sub-band.

So the cover image(stego image) is watermarked in all the sub-bands of host image by modifying the singular values of each sub-band.

The proposed methodology is implemented using the MATLAB. The simulation result is as shown in the fig 2.

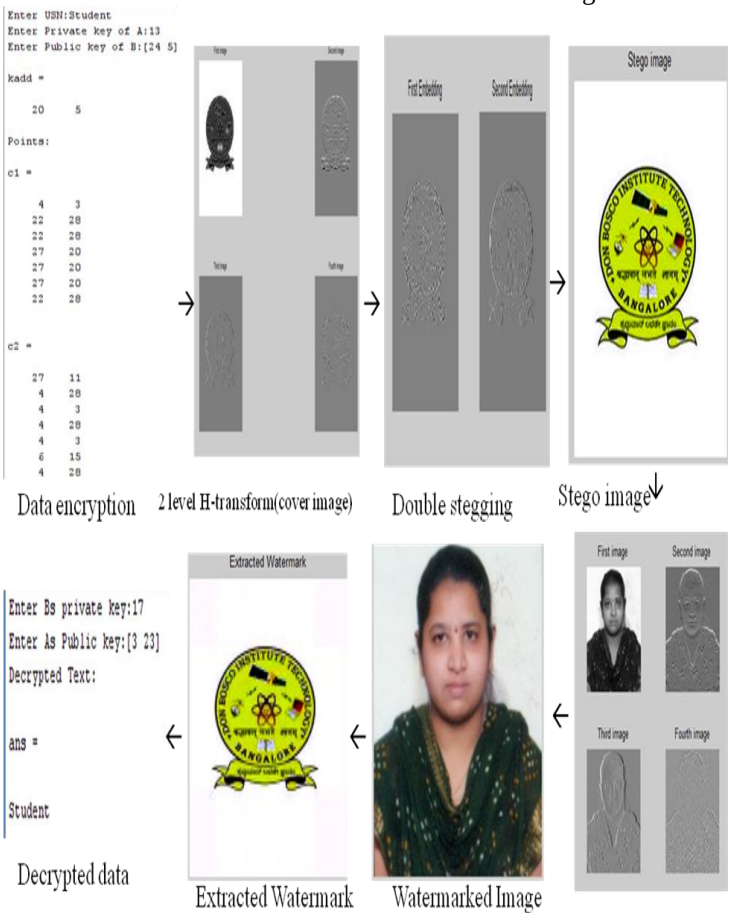

Fig 2: simulation results

IV. RESULTS

The number of doubling operations is less compared to maria method for example take character "S" in proposed method the following operations are carried out

S→$(53)_{16}$→$(5,3)_{16}$→$(5,3)_{10}$

Then calculate 5G=2(2G)+G AND 3G=(2G)+G, so the total operations are 3D+2A=5 operations. Whereas in maria method "S" = $(83)_{ASCII}$ then calculate 83G=2(2(2(2(2G)G)+G)+G and the total operations are 6D+3A=9 operations(D for doubling and A for addition) so,in proposed method the character "S" needs 5 operation where in maria method it needs 7 operations. Table 2

summarizes the operations that are required for each method to transform plain text "Student" into affine points on the EC.

Table 2 shows that the proposed method is better than maria method. In this method to transform the character "S" which has the hexadecimal ASCII value 53 into affine point on the Elliptic curve we need 5operations.wheras,in maria method the decimal ASCII value for "S" is 83 so the sender needs 9 operations to do the transformation. The total operations needed that is needed for plaintext "Hello" is 42 in proposed method and 63 in Maria method and the difference between the two methods will be increased if the size of the plaintext is increased.

Table 2. Number of doubling and addition operations for plaintext "Student"

The method	S	t	u	d	e	n	t	Total operations
Proposed method	3D + 2A	4D + 2A	4D + 3A	4D + 1A	4D + 2A	5D + 2A	4D + 2A	42
Maria method	6D + 3A	6D + 3A	6D + 4A	6D + 2A	6D + 1A	6D + 1A	6D + 4A	63

To calculate the improvement percentage for the plaintext "Student", subtract number of operations in the proposed method from number of operations in Maria method and divide by number of operations in Maria method then multiply by 100% as follows:

Improvement percentage for "Student"

$$\frac{63-42}{63} * 100\% = 33.33\%$$

As the number of doubling and addition operation reduced the computation becomes faster higher security level is provided.

V.CONCLUSION

In proposed method the security strength of the database is extended to good level because of the combination of the ECC, Double Stegging,, and SVD watermarking. because ECC is the most efficient cryptosystem with lesser key size compare to RSA algorithm. Moreover the number of doubling operations is reduced in proposed method. double stegging and SVD watermarking yields best PSNR value, increases the data security and makes the system more efficient. So. Proposed method is the powerful tool for the communication over internet in the presence of adversaries

V1 REFERENCES

[1] Victor S.Miller, Useof Elliptic Curves in Cryptography, Advances in Cryptology-CRYPTO'85 Proceedings, Springer, vol. 218, pp. 417–426, December (2000). [2] Neal Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, vol. 48, issue 177, pp. 203–209, January (1987).

[2] Neal Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, vol. 48, issue 177, pp. 203–209, January (1987)

[3] M. Bellare And P. Rogaway. "The Exact Security Of Digital Signatures-How To Sign With RSA and Rabin". In Advances In Cryptology-Eurocrypt „96, Pp. 399-416, Springer-Verlag, 1996.

[4] M. Chapman, G. Davida. "Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text". Master Thesis, Milwaukee: University of Wisconsin-Milwaukee, 1998.

[5] M. Bellare and P. Rogaway. "*Optimal* Asymmetric Encryption-How To Encrypt With RSA". In Advances In Cryptology Eurocrypt „94, Pp. 92-111, Springer-Verlag, 1994.

[6] Boruah D, Saikia M. "Implementation of ElGamal Elliptic Curve Cryptography over prime field using C". IEEE Inter- national Conference on Information Communication and embedded systems.vol.1.issue 1.2014

.[6] Katzenbeisser and Petitcolas , "Information Hiding Techniques for Stenography and Digital watermaking" Artech House, Norwood, MA. 2000.

[7]Arun Kumar Ray, Sabyasachi Padhihary, Prasanta Kumar Patra and Mihir Narayan Mohanty" Development of a New Algorithm Based on SVD for Image Watermarking" Springer India 2015 I.K. Sethi (ed.), Computational Vision and Robotics, Advances in Intelligent Systems and Computing 332.

[8]Kotagiri Ramu , Kalpana Reddy" Image Steganography in domain using double-Stegging"" Kotagiri Ramu, et al , International Journal of Research Sciences and Advanced Engineering [IJRSAE]TM Volume 2 , Issue 8, PP: 76 - 79 , OCT - DEC 2014.

[9] Vigila SMC, Muneeswaran K. A new elliptic curve cryp- tosystem for securing sensitive data applications. Interna- tional Journal of Electronic Security and Digital Forensics. 2013; 5(1):11–24.

[10] Vigila S, Muneeswaran K. Implementation of text based cryptosystem using elliptic curve cryptography. IEEE Pro- ceedings of Advanced Computing Conference; 2009.

[11] R. Balamurugan, V. Kamalakannan, D. Rahul Ganth and S. Tamilselvan, "Enhancing Security in Text Messages Using Matrix based Mapping and ElGamal Method in Elliptic Curve Cryptography", International Conference on Contemporary Computing and Informatics, IEEE, pp. 103–106, November (2014).

[12] S.Lyu and H. Farid , "Steganography using higher order image statistics , " IEEE Trans. Inf. Forens. Secur. 2006.

[13]M. Amara and A. Siad, "Elliptic Curve Cryptography and its Applications", 7th International Workshop on Systems, Signal Processing and their Applications.