Enhanced Secured Algorithm using Cryptography, Steganography and Watermarking

Sandeep Kumar U
PG Student (VLSI & Embedded System)
Dept of ECE
Sri Siddhartha Institute of Technology
Tumkur, India
Email: sundeepshekar@gmail.com

Dr. M. Z. Kurian
Dean and HOD, Dept of ECE
Sri Siddhartha Institute of Technology
Tumkur, India
Email: mzkurianvc@gmail.com

Mrs. Y. Manjula
Assistant Professor, Dept of ECE
Sri Siddhartha Institute of Technology
Tumkur, India
Email: manju.yerva@gmail.com

Abstract: Increase in the number of eavesdroppers during information exchange between the source and intended destination has indeed called for a more robust method for securing data transfer. Steganography and Cryptography are the well known and widely used techniques that manipulate the information in order cipher and hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In this proposed system, a data hiding, that is based on image steganography, cryptography and water marking is employed to secure data transfer between the source and destination. DWT (Discrete Wavelet transform) method is used to compression of image in steganography and a ECC (Elliptic Curve Cryptography) is employed to encode the message inside the image. the proposed system not only hides large volume of data in an image, but also limits the perceivable distortion that might occur in an image while processing it, and provide a strong backbone for its security.

KEYWORDS- Text, Image, DWT, ECC, Cryptography, Steganography, Watermarking,.

I. INTRODUCTION

Steganography is an art of transferring message in a way that the existence of message is concealed. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today's computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's of redundant bits. Modern steganography's goal is to keep the presence of the message undetectable from an unauthorized access.

Cryptography and Steganography are the well known and widely used techniques that manipulate information in order cipher and hide their existence respectively. Cryptography scrambles a message so that it cannot be understood; the Steganography hides the message that it cannot be seen. And Watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal, known as watermark, can be used to identify the owner, to authenticate the content, and to trace illegal copies of the work. Combining these three methods together for the purpose of developing a system that will improve the confidentiality and security of the message. According to [1], the power of steganography is in hiding the secret message by obscurity, and hiding its existence in a non-secret file. In that, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence. The success of steganography technique depends entirely on the ability to hide the message such that an observer would not suspect its existence, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this technique is done will differ for the specific media that are used to hide the secret information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier it becomes detectable.

Basically, the purpose of cryptography, steganography and watermarking is to provide secret communication. Cryptography is used to conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography uses two main styles or forms of encrypting data; symmetrical and asymmetrical. Symmetrical encryptions use the same key for encryption as they do for decryption. While asymmetrical encryptions use the different keys for encryption and decryption. In this paper, a text data is used for cryptography and a more powerful efficient method ECC (elliptic curve cryptography) was used, which is an asymmetrical one employed for encryption and decryption of text message. In this proposed method, the group of points on elliptic curves over finite fields can be used for public-key cryptography. The principal operation in elliptic curve cryptographic system is point multiplication. According to [1], the two most common methods used for hiding information inside a picture, audio and video files are LSB (Least Significant Bit) and Injection. In this paper, an image medium was used for Steganography and a more powerful modified DWT (Discrete Wavelet Transform) was employed for encoding the message into the image file. The Discrete Wavelet Transform, which is based on sub-band coding, is found to be yield a fast computation of wavelet transform.

Watermarking technology is used for copyright protection of images, audios and videos. A digital watermark is a piece of information which is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it cannot be separable from its original data. This piece of information known as watermark, a tag, or a 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.

II. RELATED WORK

"Hiding the text information using Steganography" by M.Grace Vennice, Prof.T.V.Rao, M.Swapna and Prof.J.Sasi kiran [2] presented a various existing text-based steganography techniques, an overview of text steganography and a brief history of steganography. Also highlighted the problems present in the text steganography and issues with existing solutions.

"A secured image based Steganography and Cryptography with Watermarking" by Sarita Poonia, Mamtesh Nokhwal, and Ajay Shankar [3] described the techniques used for cryptography and steganography, and explained the digital watermarking process. Presented the basic types of cryptography ie., symmetrical and asymmetrical and least significant bit approach used in steganography.

"Efficient Data Hiding System using Cryptography and Steganography" by Abikoye Oluwakemi, Adewole Kayode S and Oladipupo Ayotunde J [4] presented a data hiding system that is based on audio steganography, and proposed cryptographic technique to secure the data transfer between the source and destination. Audio medium is used and a LSB (least significant bit) algorithm is employed to encode the message inside the audio file.

"Optimal asymmetric encryption- How to encrypt with RSA" by M. Bellare and P. Rogaway [5] exhibits an encryption scheme for which (i) any string x of length slightly less than k bits can be encrypted as f(rx), where rx is a simple probabilistic encoding of x depending on the hash function; and (ii) the scheme can be proven semantically secure assuming the hash function is ideal. Moreover, a slightly enhanced scheme is shown to have the property that the adversary can create cipher texts only of strings for which she/he knows the corresponding plain texts such a scheme is not only semantically secure, but also non-malleable and secure against chosen-cipher text attack.

"Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations" by Gustavo D. Sutter and Jean-Pierre Deschamps [13] presented the design of a new high-speed point multiplier for elliptic curve cryptography using either field programmable gate array or application-specified integrated circuit technology. Different levels of digit-serial computation were applied to the data path of Galois field (GF) multiplication and division to explore the resulting performances and find out an optimal digit size.

"A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphisms" by Reza Azarderakhsh and Koray Karabina [14] described a new double point multiplication algorithm based on differential addition chains. Proposed scheme has a uniform structure and has some degree of built-in resistance against side channel analysis attacks. Deploying scheme in a hardware implementation of single point multiplication on binary elliptic curves with efficiently computable endomorphism's.

"Elliptic Curve Cryptography in Practice", by Joppe W. Bos1, J. Alex Halderman2, Michael Naehrig1, and Eric Wustrow2 [15] presented a review of elliptic curve cryptography (ECC), that is presently used in practice today. In order to reveal

unique mistakes and vulnerabilities that arise in implementations of ECC. Proposed four popular protocols that make use of this type of public-key cryptography: Bitcoin, secure shell (SSH), transport layer security (TLS), and the Austrian e-ID card. And pleased to observe that about 1 in 10 systems support ECC across the TLS and SSH protocols.

III. PROPOSED SYSTEM

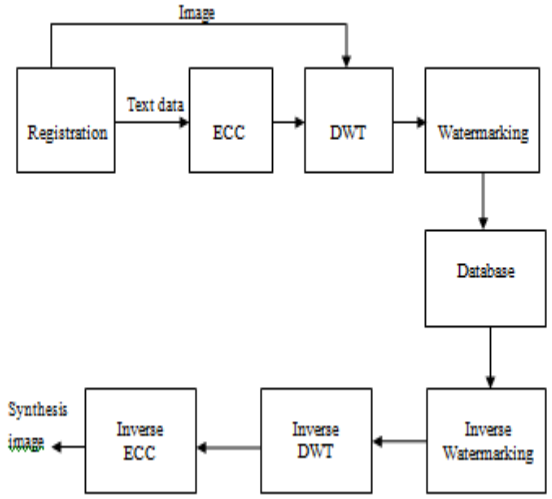

Fig 1: Block diagram of secured image

In Cryptographic system we basically used the elliptic curve cryptography (ECC) technique.
Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. The entire security of ECC depends on the ability to compute point-multiplication. The size of the elliptic curve determines the difficulty of the problem. The primary benefit of ECC is a smaller key size, reducing storage and transmission requirements than RSA-based system. For current cryptographic purpose, an elliptic curve is a plane curve which consists of the points satisfying the equation

$$y^3 = x^3 + ax + c. \qquad (1)$$

In steganographic system we used the Discrete Wavelet Transform (DWT) technique on cover image.
Which include the following steps in this case:-
1. The image is broken into data units each of them consists of 8x8 block of pixels.
2. Working from top-left to bottom-right of the cover image, DWT is applied to each pixel of each data unit.
3. After applying DWT, one DWT coefficient is generated for each pixel in data unit.
4. Each DWT coefficient is then quantized.
5. The LSB of binary equivalent the quantized DWT coefficient can be replaced by a bit from secret message.
6. Encoding is then applied to each modified quantized DWT coefficient to produce compressed image.

Watermarking is used to signify ownership and source authenticity. The aim of watermark is to mark digital data permanently and unalterably, so that the source as well as the intended recipient of the digital work is known. Watermarks can be visible or invisible. In this proposed system, we uses invisible water marking method. Where in invisible watermarks a digital label is used to signify the ownership and authentication.

IV. METHODOLOGY

Elliptic Curve Cryptography(ECC):
Elliptic curve cryptography is gaining popularity because it offers similar security to traditional systems, such as Ron Rivest, Adi Shamir and Leonard Adleman (RSA), but with significantly smaller key lengths. It is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The ECC method was employed during encryption of text data, the below flow chart shows the steps involved in generating public and private key to encrypt and decrypt the data respectively.

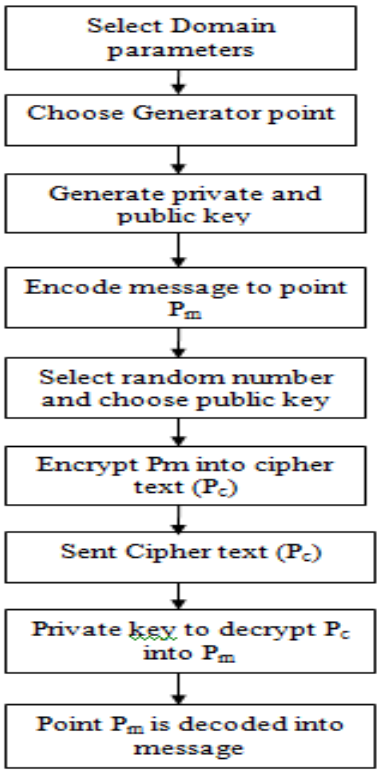

Fig 2 : Flow chart of cryptographic implementation

To use ECC all parties must agree on all the elements defining the elliptic curve, that is, the domain parameters of the scheme. The field is defined by p in the prime case and the pair of m and f in the binary case. The elliptic curve is defined by the constants a and b used in its defining equation. Finally, the cyclic subgroup is defined by its generator point G. For cryptographic application the order of G, that is the smallest value of n such that nG = 0 is a prime number.

V. RESULTS AND DISCUSSION

The proposed system was developed using MAT Lab programming. During execution, the main class displays the following preliminary operations: point addition, point doubling and point multiplication.

Point addition: This step uses two distinct points such that to generate slope of line.

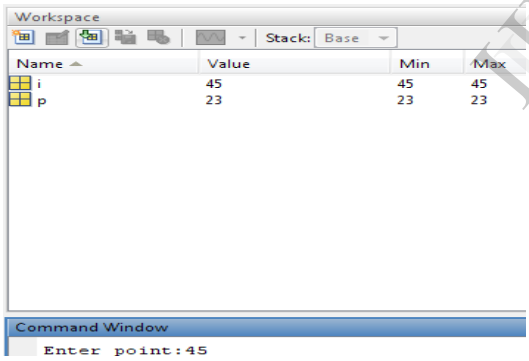

Fig 3: Distinct point generation

Point doubling: This is the next step of point addition which determines the point of coordinates to be assign with the elliptic curve

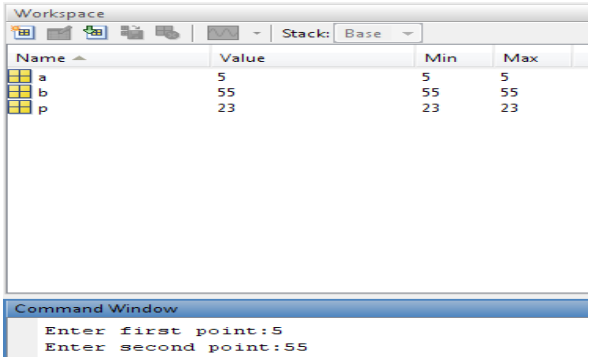

Fig 4: Parameters choosen with elliptic curve

Point multiplication:
The point multiplication uses both point addition and point doubling. Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain anther point Q on the curve. i.e. to find Q = kP

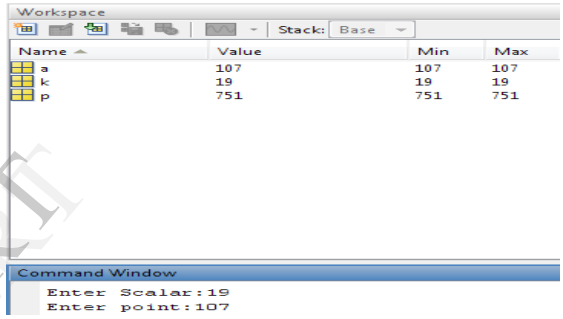

Fig 5: Cipher text assign to scalar points

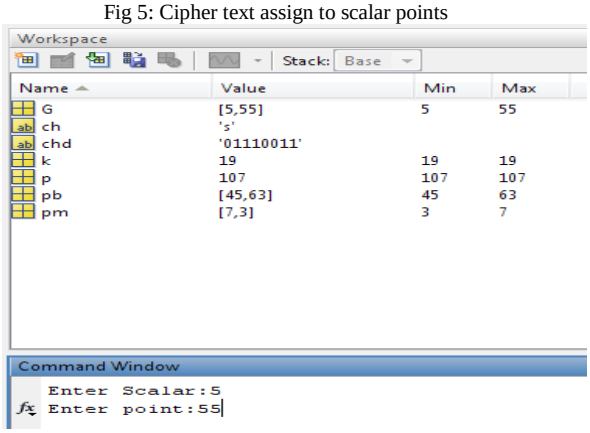

Fig 6: Private key generation to extract the data

VI. CONCLUSION

A comparative study from the survey of previous methodologies about the cryptography, steganography and watermarking has been made. High performance architecture for point multiplication, the key operation of ECC, has been proposed. In the next section, we consider the effectiveness of DWT (Discrete Wavelet Transform) employed to encode the message inside

the image file and watermarking technology for authenticating. The system therefore, make its security more robust.

VII. REFERENCES

[1] Sridevi R, Damodaram A, and Narasimham S. "*Efficient Method of Audio Steganography By Modified LSB Algorithm and Strong Encryption Key With Enhanced Security.* " Journal of Tretical and Applied Information Technology, pp. 768-771.

[2] M.Grace Vennice, Prof.Tv.Rao, M.Swapna and Prof.J.Sasi kiran. "*Hiding the text information using Steganography*." International national journal of Engineering Research and Application (IJERA),ISSN: 2248-9622 Vol. 2, Issue-1, jan-Feb 2012, pp.126-131.

[3] Sarita Poonia, Mamtesh Nokhwal, and Ajay Shankar. "*A Secured Image based Steganography and Cryptography with Watermarking"*. International Journal of Engineering Science and Engineering (IJESE) ISSN: 2319-6378, Vol. 1, Issue-8, June 2013.

[4] Abikoye Oluwakemi, Adewole Kayode S and Oladipupo Ayotunde J *"Efficient Data Hiding System using Cryptography and Steganography"* International Journal of Applied Information Systems (IJAIS)- ISSN: 2249-0868, Vol.4- No.11, December 2012

[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] 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.

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

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

[9] N .Provos and P. Honeyman, "*Hide and Seek: An introduction to Steganography*," IEEE Security & Privacy Journal 2003.

[10] N .Provos, "*Defending Against Statistical Steganography*," Proc 10th USENEX Security Symposium 2005.

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

[12] L. Reyzen and S.Russell, "*More efficient provably secure steganography*" 2007.

[13] Gustavo D. Sutter, Jean-Pierre Deschamps, and José Luis Imaña "*Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations*" IEEE transactions on industrial electronics, vol. 60, no. 1, January 2013.

[14] Reza Azarderakhsh and Koray Karabina "*A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphism.s*"

[15] Joppe W. Bos1, J. Alex Halderman2, Michael Naehrig1, and Eric Wustrow2, "*Elliptic Curve Cryptography in Practice*", Microsoft Research 2 University of Michigan