ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

A Secured Algorithm Based On ECC and DWT with Watermarking

Sandeep kumar U, Y.Manjula, Dr.K.B.Shivakumar, Dr.M.Z.Kurian

M.Tech Student (VLSI and Embedded Systems), Dept of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Assistant Professor, Dept of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Professor, Dept of Tele-Communication & Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Dean & Head, Dept of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.

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. Due to increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. In this ECC-DWT processor along with watermarking a secure image algorithm is proposed. The group of rational points on elliptic curves over finite fields can be used for public-key cryptography. The elliptic curve cryptography (ECC) has been identified and employed as an efficient and suitable scheme for public key cryptographic systems. Image is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the image and is applied during discrete wavelet transform (DWT) on coverage 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: DWT, ECC, Security, Watermarking

I. INTRODUCTION

In the past, people used hidden tattoos or invisible ink to convey steganographic content. In this paper we proposed the various techniques used during cryptographic and steganographic algorithms. The principal operation in elliptic curve cryptographic systems is point multiplication based on Fermat's little theorem. Basically, 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.

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) has been 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

II. RELATED WORK

In [2] authors 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.

In [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.

In [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.

In [9] 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.

In [11] presented a high speed and efficient pipelined partially serial architecture to enhance the speed and area efficiency.

III. PROPOSED SYSTEM

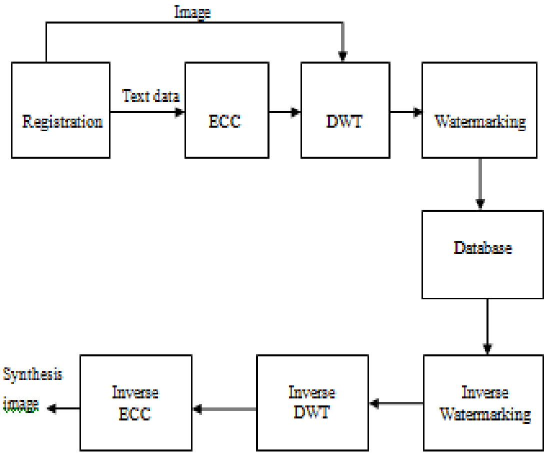


Fig 1: Block diagram of secured image

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

$$y^2 = x^3 + ax + b \bmod p. \qquad \text{eq. (1)}$$

In steganographic system we applying LSB technique during Discrete Wavelet Transform (DWT) on cover image.

The following steps are followed 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.
When the embedded data's bits are substituted into the least significant bits (LSB's) location it will have little no effect on the image appearance to the human eye.

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.

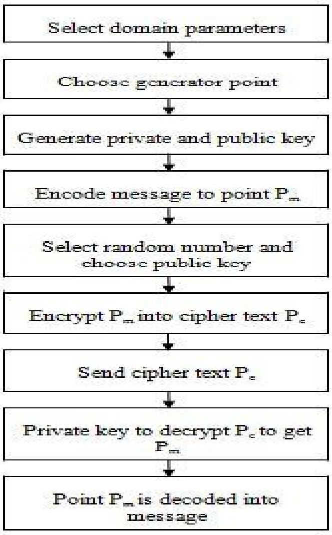

Select domain parameters
Choose generator point
Generate private and public key
Encode message to point P_m
Select random number and choose public key
Encrypt P_m into cipher text P_c
Send cipher text P_c
Private key to decrypt P_c to get P_m
Point P_m is decoded into message

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. PSEUDO CODE

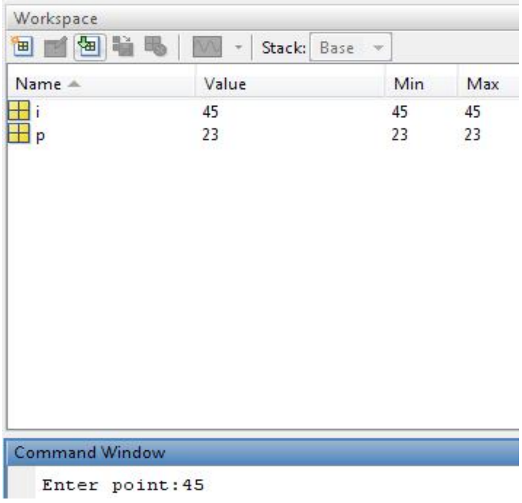
```
Step 1:  Generate domain parameters.
Step 2:  Calculate the generator point using eq. (1).
Step 3:  Generate private key and public key.
Step 4:  Encode the message to generator point.
Step 5:  Choose public key to encrypt the message and send as cipher text.
Step 6:  Use private key to decrypt the cipher text.
Step 7:  Message in generator point is decoded.
```

Step 8: End.

VI. SIMULATION RESULT

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.

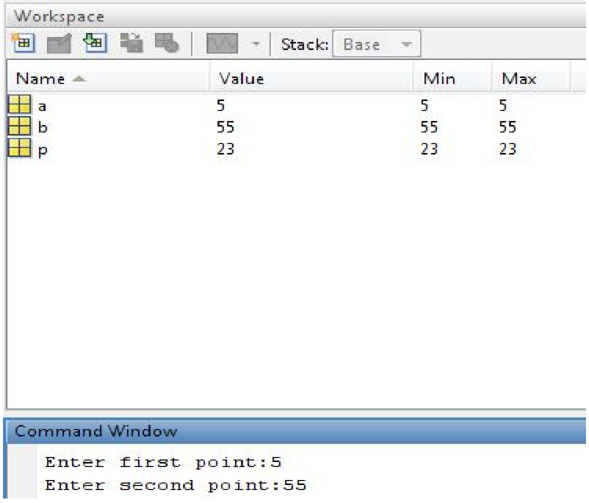
In fig 3 Point addition uses two distinct points such that to generate slope of line. The Point doubling used in fig 4 is the next step of point addition which determines the point of coordinates to be assign with the elliptic curve. The point multiplication uses both point addition and point doubling. 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 in fig 5 and generate d binary code for the character ‘S’ and provides the private key to extract the message as shown in fig 6.



Name	Value	Min	Max
i	45	45	45
p	23	23	23

```
Enter point:45
```

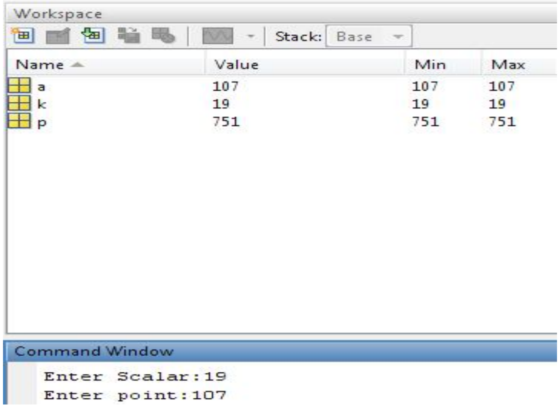
Fig 3: Distinct point generation



Name	Value	Min	Max
a	5	5	5
b	55	55	55
p	23	23	23

```
Enter first point:5
Enter second point:55
```

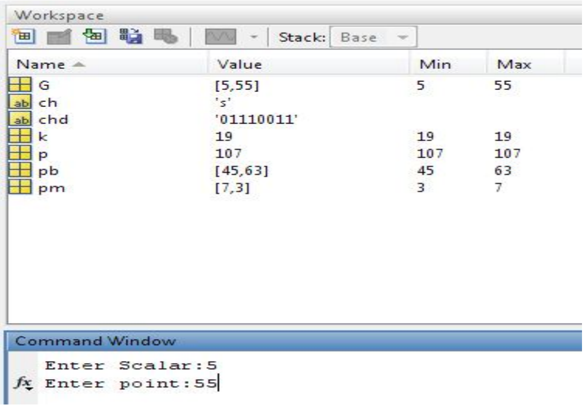
Fig 4: Parameters choosen with elliptic curve



Name	Value	Min	Max
a	107	107	107
k	19	19	19
p	751	751	751

```
Enter Scalar:19
Enter point:107
```

Fig 5: Cipher text assign to scalar points



Name	Value	Min	Max
G	[5,55]	5	55
ch	's'		
chd	'01110011'		
k	19	19	19
p	107	107	107
pb	[45,63]	45	63
pm	[7,3]	3	7

```
Enter Scalar:5
Enter point:55
```

Fig 6: Public key generation to extract the data

VII. Conclusion and Future Work

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.

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 Theoretical and Applied Information Technology (JATIT), Vol.5, pp.768-771, 2005.
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), Vol.1, pp.66-70, 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), Vol.4, pp.6-11, 2012.
5. M. Bellare and P. Rogaway. "Optimal Asymmetric Encryption-How To Encrypt With RSA". International conference on advances in Cryptography-Eurocrypt techniques, Vol.950, pp.92-111, 1995.
6. M. Bellare And P. Rogaway. "The Exact Security Of Digital Signatures-How To Sign With RSA and Rabin". International Conference on Theory ans Application of Cryptographic Techniques, Vol.96, pp.399-416, 1996.
7. N .Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE transaction on Security & Privacy Journal, Vol.1, pp.32-44, 2003.
8. S.Lyu and H.Farid, "Steganography using higher order image statistics," IEEE Transaction on Information Forensics and Security, Vol.1, pp.111-119, 2006.
9. 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, pp.217-225, 2013.
10. Reza Azarderakhsh and Koray Karabina "A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphisms". IEEE Transactions on Computers society, Vol.62, pp.1-7, 2013.
11. Sugreev Kaur and Rajesh Mehra, "High Speed and Area Efficient 2D DWT Processor Based Image Compression", Signal and Image Processing: An International Jpournal (SIPIJ), Vol.1, pp.22-31, 2010.

BIOGRAPHY

Sandeep kumar u is a MTech Student (VLSI and Embedded Systems), Dept of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India. His area of interest includes VLSI Design and Image processing.

Mrs. Y. Manjula MTech is an Assistant Professor, Dept of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India. Her area of interest is Digital Electronics.

Dr. K. B. Shivakumar ME, MBA, MPhil, PhD is a Professor, Dept of Tele-Communication & Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India. His area of interest includes Image processing, Cryptography and Steganography.

Dr. M. Z. Kurian MTech, PhD, MISTE, MIEEE is a Dean & Head, Dept of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India. His area of interest is Software Engineering.