Implementation of ECC and ECDSA for Image Security

Dhanashree Toradmalle
Assistant Professor, Department of Information Technology
Shah & Anchor Kutchhi Engineering College, Chembur.
Mumbai, India
dhanashree.kt@gmail.com

Varsha Sonigara
UG Student, Department of Information Technology
Shah & Anchor Kutchhi Engineering College, Chembur.
Mumbai, India
varshasonigara2017@gmail.com

Kiran Singh
UG Student, Department of Information Technology
Shah & Anchor Kutchhi Engineering College, Chembur.
Mumbai, India
singhkiran1805@gmail.com

Omkar Kakade
UG Student, Department of Information Technology
Shah & Anchor Kutchhi Engineering College, Chembur.
Mumbai, India
omkarkakade2017@gmail.com

Krishnachandra Panigrahy
UG Student, Department of Information Technology
Shah & Anchor Kutchhi Engineering College, Chembur.
Mumbai, India
krishnachandrapanigrahy2017@gmail.com

***Abstract*—** the use of digital data has been increase over the past decade which has led to the evolution of digital world. With this evolution the use of data such as text, images and other multimedia for communication purpose over network needs to be secured during transmission. Images been the most extensively used digital data throughout the world, there is a need for the security of images, so that the confidentiality, integrity and availability of the data is maintained. There is various cryptography techniques used for image security of which the asymmetric cryptography is most extensively used for securing data transmission. This paper discusses about Elliptic Curve Cryptography an asymmetric public key cryptography method for image transmission. With security it is also crucial to address the computational aspects of the cryptography methods used for securing images. The paper proposes an Image encryption and decryption method using ECC. Integrity of image transmission is achieved by using Elliptic Curve Digital Signature Algorithm (ECDSA) and also considering computational aspects at each stage.

Keywords-*component; Asymmetric Key Cryptography, Elliptic Curve Cryptography, ECDSA, Image Security*

*****

I. INTRODUCTION

With the ascent in online exchange, the utilization of wireless network devices has increased. It is a decent stride towards world been advanced, however there might be certain security threats to these network devices requesting a stringent security framework. In this manner giving security to these systems will guarantee that they accomplish the desired security objectives. The widely known security frameworks include the utilization of asymmetric cryptographic techniques, for example, RSA, Diffie-Hellman to give security of which RSA is the most broadly utilized method. But RSA has a disadvantage of increased bit length thus increasing the key size which needs more computational time and makes the system a bit inefficient.

To overcome this drawback of RSA we use Elliptic key cryptography. The concept of Elliptic curve cryptography was introduced by Neal Koblitz and Victor S. Miller. ECC has comparatively smaller key size which takes less computational time. It is also preferred because of its non-traceable trapdoor function. Elliptic Curve algorithms for signature and key exchange require shorter keys for security. With such keys, ECDSA signatures and ECDH are significantly faster than RSA signatures. Therefore ECC can be used in environment where processing power, time and storage are constrained.

II. REVIEW OF LITERATURE

Darrel Hankerson, Alfred Menezes and Vanstone introduced different cryptography techniques. The author explained why ECC is considered over other cryptography techniques. He also compared other techniques with ECC and concluded ECC to be a better alternative for encryption process. The author also explains the traditional approach for ECDSA which uses inversion operation for signing and verification [2]. On the other hand Laiphrakpam Dolendro Singh explained the concept of pixel grouping operation for pixel encoding followed by ECC image encryption [3]. Noor Dhia Kadhm Al-Shakarchy proposes a system which uses a textual algorithm to encode and decode digital color images [4]. It discusses about various ciphering algorithms which includes Hill Cipher, Arnold Cat Map System so as to obtain a cipher image. Ravi Kishore Kodali proposes ECC using Koblitz encoding method which is used to encode images [5]. The author concludes that koblitz encoding method provides more security to ECC rather than other ciphering techniques. Nikita Gupta proposes a system which includes the encoding of a single pixel individually which a static mapping needs table for mapping the pixels, which is very time consuming [6]. Tao Long describes two improved versions of digital signature schemes based on ECC [7]. This scheme eliminates the use of inversion operation by some modifications in traditional ECDSA. The author in [8]

talks about the different variants of DSA and compares them to find the most efficient variant among them.

TABLE I – Key Comparison [6]

Symmetric Key Size	RSA and Diffie-Hellman Key Size	ECC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

.

III. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography involves a public and a private key for the process of encryption and decryption. The elliptic curve is a curve which is symmetric about the x-axis and its equation consists of two variables and coefficients. The general equation for an elliptic curve is given by

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

Where a, b must satisfy the following condition:

$$4a^3+27b^2 \neq 0(\text{mod } p) \quad (2)$$

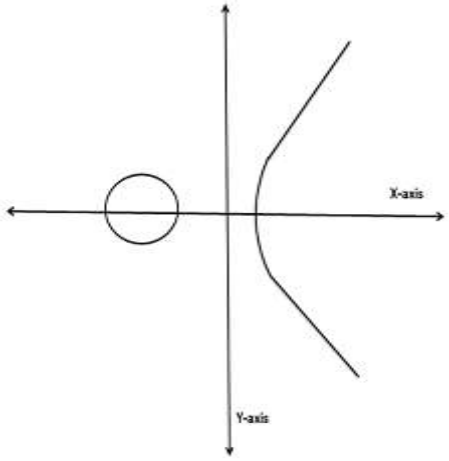

Fig 1 : Elliptic Curve

A. ECC Curve Parameters

There are certain parameters which are essential for the above ECC functions to work. These parameters are defined as follows:

i. a, b: The two coefficients which define the curve.
ii. Generator base point (G): This point is use to define the start of the curve.
iii. Order of curve generator Point (N): It is the cyclic order of the base point.
iv. Prime field (Fp): 'P' a prime number is used to define a field in which the curve operation.

B. Point Addition

There is a rule, called the chord-and tangent rule, for adding two points on an elliptic curve E(Fp) to give a third elliptic curve point. The addition rule is best explained geometrically. Let P = (X_1, Y_1) and Q = (X_2, Y_2) be two distinct points on an elliptic curve E. Then the sum of P and Q is denoted by R = (X_3, Y_3). First draw a line through P and Q; this line intersects the elliptic curve at a third point, then R is the reflection of this point in the x axis. Mathematically point addition is given by [3]:

$$P(X_1, Y_1) + Q(X_2, Y_2) = R(X_3, Y_3) \quad (3)$$

$$X_3 = (\lambda^2 - X_1 - X_2) \text{ mod } p$$

$$Y_3 = (\lambda (X_1 - X_3) - Y_1) \text{ mod } p$$

$$\text{WHERE, } \lambda = (Y_2 - Y_1) / (X_2 - X_1) \text{ mod } p$$

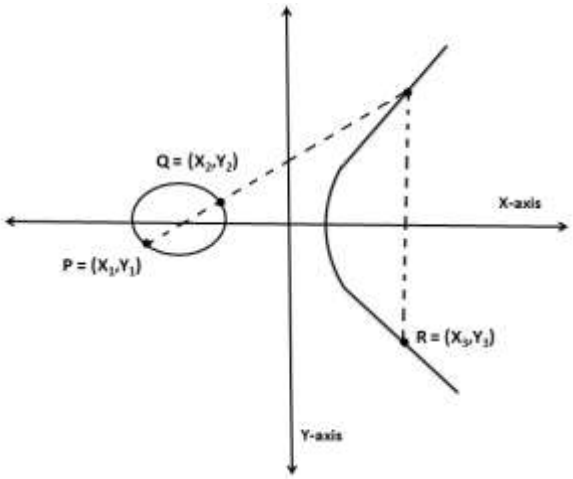

Fig 2 : Point Addition

C. Point Doubling

If a tangent is drawn through a point P (x_1, y_1) on the elliptic curve then the double of the point P(x_1 , y_1) is a point R(x_3 , y_3) which is a reflection of the point obtained by the intersection formed through the tangent drawn at point P (x_1 , y_1). Mathematically it is given by [3]:

$$P(X_1, Y_1) + P(X_1, Y_1) = R(X_3, Y_3) \quad (4)$$

$$X_3 = (\lambda^2 - 2X_1) \text{ mod } p$$

$$Y_3 = (\lambda(X_1 - X_3) - Y_1) \text{ mod } p$$

$$\text{WHERE, } \lambda= (3X_1^2 + a) / (2Y_1) \text{ mod } p$$

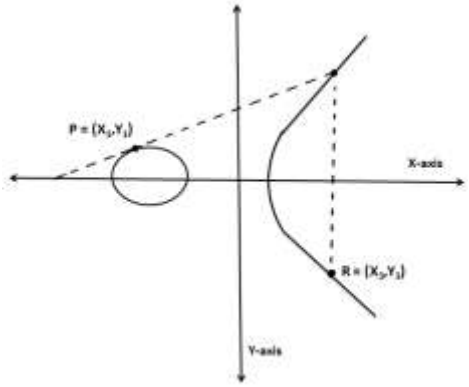

Fig 3 : Point Doubling

D. Point Subtraction

To perform point subtraction, get a mirror coordinate of the subtracted point along x-axis and perform point addition on

 ISSN: 2321-8169
734 – 737

the resulting coordinate and the other coordinate. Mathematically it is given by [3]:

$$P(X_1, Y_1) - Q(X_2, Y_2) = P(X_1, Y_1) + Q(X_2, -Y_2) \quad (5)$$

IV. Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm(DSA). A digital signature is a number dependent on some secret known only to the signer (the signer's private key), and, additionally, on the contents of the message being signed. Signatures must be verifiable to check whether an entity signed a document. Elliptic Curve Digital Signature Algorithm (ECDSA) is based on IEEE 1363 standard.

V. Approched Algorithm

A. Key Pairs

ECC uses a public and a private key for encryption and decryption. The public key of the receiver denoted by (Rx, Ry) is used for the encryption of the image whereas the private key of the receiver denoted by Rp is used for the decryption process. The private key of the sender is taken as Sp and the public key is denoted by (Sx, Sy).

B. Sender Side

1. An image as an input is been accepted.
2. The Koblitz encoding [5] method is been applied to the input image so as to obtain an encoded image. .
3. The encoded image is further encrypted using the ECC encryption process which uses the public key (Rx, Ry) of the receiver.
4. The hash key value is been generated for the encrypted image.
5. Using the sender's private key Sp the above encrypted image is digitally signed.
6. The digital signature algorithm generates the output (R, S) and this is send along with the encrypted image M as the message (M, R, S).

C. Receiver Side

1. The message is been received in form of (M, R, S) where M is the cipher image, R and S are the output of digital signature.
2. The hash value for the cipher image is been calculated.
3. The digital signature is verified by the receiver at the receiver end using the sender's public key (Sx, Sy).
4. If the signature is verified properly, go to step 5 else to step 7.
5. The receiver decodes the image using the Koblitz decoding method [5].
6. The decoded image is further decrypted using the ECC decryption process which uses the private key of the Receiver Rp.
7. Image cannot be decrypted.

D. Encryption Process

A random number 'k' is generated and this 'k' is doubled with generator point of the curve 'G' so as to obtain C1.

$$C1 = k.G \quad (6)$$

Then, the encryption process uses the point addition function, which takes the encoded point and the public key of the receiver (Rx, Ry) as input, which gives the cipher image point,

$$C2 = (X, Y) + (Rx, Ry) \quad (7)$$

The final output of the encryption process is (C1, C2).

E. Decryption Process

The decryption process uses private key of the receiver Rp to obtain the original image. The C1 cipher is doubled with the private key (Rp) of the receiver hence we get decoded point

$$DC1 = Rp.\ C1 \quad (8)$$

Then the point subtraction function of ECC which is reverse function for point addition is performed. Here the cipher C2 is subtracted from (7) so as to obtain the original image point,

$$(X, Y) = C2 - DC1 \quad (9)$$

The final output of the decryption process (X, Y) that is original image pixel.

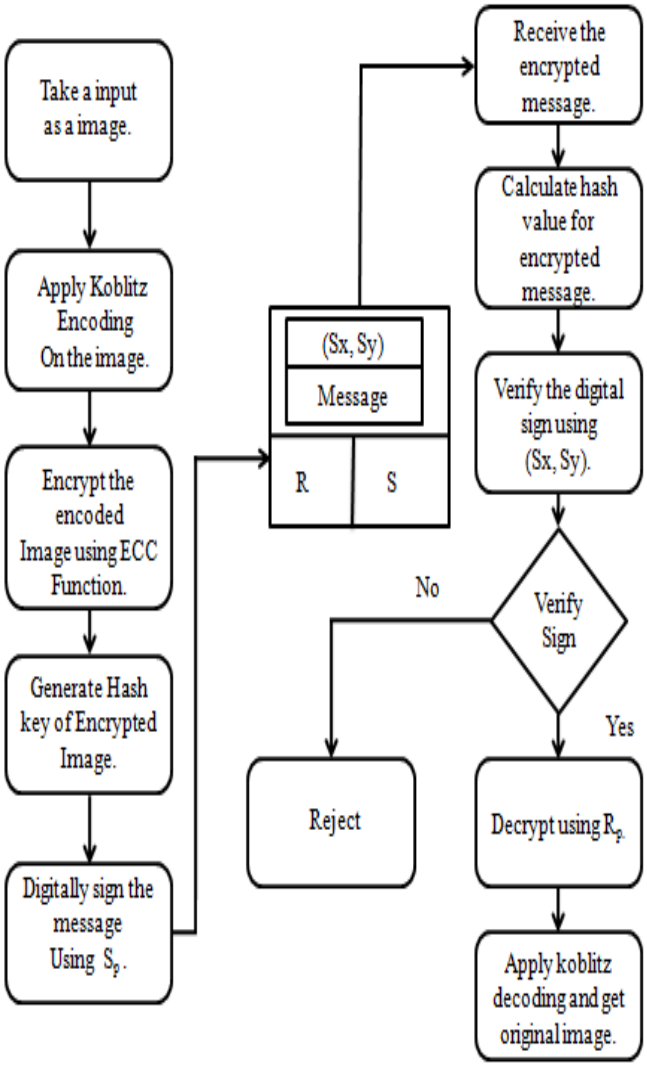

Fig 4 : Sender and Receiver working.

F. ECDSA Signature Generation

1. Select kϵ_R [1, n-1].
2. Compute k.G=(X_1, Y_1).
3. Compute R= X_1 mod n. If r=0 then go to step 1.
4. Compute e=H (m).
5. Compute S=k^{-1}(e+dr) mod n. If s=0 then go to step 1.
6. Return(R, S).

G. ECDSA Signature verification

1. Verify that r and s are integers in the interval [1, n-1]. If any verification fails then return ("Reject the signature).
2. Compute e=H (m).
3. Calculate X=(X_2,Y_2) = e.S^{-1}G + R.S^{-1}Q
4. V= X_2 mod n.

If V=R accept.

VI. APPROACHED SYSTEM OUTPUTS

TABLE II – Time Complexities for standard images

Image Name	Size	Encryption	Decryption	Signature	Verification
mandril_gray.jpg	512X512	0.125	0.875	0.047	0.015
lena_gray_512.jpg	512X512	0.11	0.672	0.016	0.031
lake.jpg	512X512	0.203	1.359	0.016	0.016
peppers_gray.jpg	512X512	0.109	0.672	0.015	0.047
lena_gray_256.jpg	256X256	0.117	0.331	0.013	0.028

Fig 5: Input image

Fig 6: Cipher image

Fig 7: Output image

VII. CONCLUSION

The proposed system is an approach that uses ECC for providing Image Security. ECC uses considerably smaller key sizes than other public key cryptosystems like RSA. The system incorporates the implementation technique for encryption and decryption of the image. Furthermore, the ECDSA signing and verification algorithms provide authenticity and integrity of images. The time complexities for the encryption, decryption process and the signing, verification process are computed and analysed for standard images of two different image sizes. As seen, the complexities depend on the size of image as well as the input parameters for the ECC.

REFERENCES

[1] Williams Stallings, "Cryptography and Network Security", 4th Edition, Prentice Hall, Pearson.

[2] Darrel Hankerson, Alfrared Menzes, Scott Vanstone, "Guide to Elliptic curve cryptography", Springer.

[3] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, "Image encryption using elliptic curve cryptography", ScienceDirect, Eleventh International Multi-conference Information processing.

[4] Noor Dhia Kadhm Al-Shakarchy, Hiba Jabbar Al-Eqabie, Huda Fawzi, Al-Shahad, "Classical Image Encryption and Decryption", IJCR.

[5] Ravi Kishore Kodali and Prof. N.V.S. Narasimha Sarma, "ECC implementing using Koblitz's Encoding", Department of Electronics and Communication Engineering, National Institute of Technology, Warangal.

[6] Nikita Gupta, Vikas Kundu, Neha Kurra, Shivani Sharma, Bhagyashree Pal, "Elliptic curve cryptography for ciphering images", IEEE, 978-1-4799-7678-2/15, 2015.

[7] Tao LONG, "Two improvements to Digital Signature Scheme based on elliptic curve cryptosystem", International Workshop on Information Security and Application(2009).

[8] Greeshma Sarath, Devesh Jinwala and Sankita Patel, "A survey on Elliptic Curve Digital Signature Algorithm and it's Variants", Department of Computer Engineering SVNIT, Surat.