Indian Journal of Science and Technology, *Vol 8(26), DOI: 10.17485/ijst/2015/v8i26/81185, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Image Security using ECC Approach

Srinivasan Nagaraj[1]* and G. S. V. P. Raju[2]

[1]Department of CSE, GMR Institute of Technology, Rajam - 532 127, Andhra Pradesh, India; sri.mtech04@gmail.com
[2]Department of CS and ST, Andhra University, Vishakapatnam - 530003, Andhra Pradesh, India; gsvpraju2011@yahoo.com

Abstract

Objectives: The role of digital images are vast in todays trends and it is exposed to illicit access, modifications that must needs confidentiality during the stages of data archival and communication[1], systems, wireless devices. In order to facilitate secret communication, image encryption have bring into being a significant place in both public and private services like as military supervision, health systems, financial services like online trading and video conferencing and so on. Some methods are proposed on the image encryption which they include the Paper[2] have developed a method for A Chaotic Key Based Algorithm (CKBA) to change the pixel values of the plain-image. In [3] have developed a protocol for random combinational image encryption approach with bit, pixel and block permutations Paper[4] proposed a technique to encrypt an image for secure transmission using the digital signature of the image. **Methods:** The proposed work is developed that provides secured authentication to integrate the image encryption with Elliptic Curve Cryptography to provide security. In this work, transformation operation of the matrix operations are performed on the original image matrix and the transformed image is further encrypted with the help of a key sequence which is generated from the elliptic Curve. The encrypted image will be authenticated using Elliptic Curve Diffie Helman (ECDH) key exchange algorithm[5] and finally decrypted by using the key generated from the chosen elliptic curve and then we perform the reverse transformations on the matrix obtained . So after decryption process to acquire the original image. **Findings:** In this work we can get better security to image ecryption by application of ECC with matrix operations performed on image data. Because ECC has the well attention of researchers and robust mathematical development and top security among the former existing algorithms. As a result Elliptic Curve Cryptography for image data is developed to meet the current security needs. **Application:** To transmit securely image data over the wireless channels and systems and so on. Currently this work was currently developed in an ad-hoc fashion and it can be further improved with ECC binary field and various measures of security that includes different attacks.

Keywords: ECDH and Elliptic–Curves, Image-Decry, Imge-Encryption, Transformation-Operations

1. Introduction

Information security can be defined to be the field of research that aims at defending information from malicious attackers as still allows legal users to manipulate data.

There are many different aspects of security that includes various threats and cryptography is not alone sufficient by itself. The following are some specific security requirements which including:

1.1 Authentication

It provides that the authenticity of one entity to allow or not to allow access of resources.

1.2 Confidentiality

In this, that the message cannot be modified by anyone except the intended receiver.

*Author for correspondence

1.3 Integrity and Non-repudiation.

Method of protecting information from unauthorized access, use, revealing, perturbation and modification and scrutiny and so on. It is recognized that can be used in spite of the form that the data can be achieved and that the authentication plays a major role in the security field[5]. The awareness is the vital role in today's world. People are demanding for a new way to the security that should be more reliable and authentic.

The idea of information security leads to the evolution of Cryptography and it is the science of keep the information to be secure. It must includes the encryption process, decryption techniques of images. There are quite a few well recognized cryptographic algorithms exist. The importance part of the cryptography is the "key" used for encrypting and decrypting of the information. The very familiar cryptographic methods are to be public and though some organizations think in having the methods a max out secret. Digital images are very usage data type with wide spread range of use and many users are interesting to implement content protection methods on their images to keep it from preview and its direction. So lots of applications exist based on image. The very important task of images at industrial process intrested into a resource. So its need to keep confidential images data from unauthorized access.

Cryptography is the science of hiding information which can be revealed only by genuine users. It is used to provide the privacy for transmitted data over an unsecure channel and prevent eavesdropping and data tampering and there is another countryside called cryptanalysis which is concerned with attacking and decrypting with these ciphering data. A copious cryptography schemes were developed and used for securing data; some use the shared key cryptography and others use the Public Key Cryptography (PKC). The shared key cryptography is a system which uses only one key by both sender and receiver for the purpose of encrypting and decrypting messages. The public cryptography use two separate keys so called as private-key, public-keys.

As compared to the shared key cryptography, Public Key Cryptography are somewhat slow. But the applications of Public Key Cryptography systems in the company of the shared key cryptography to get the best of both. In particular, The Public Key Cryptography has many advantages over the shared key; among others, it increases the security and convenience where distributing the private key to other party is may not compulsory. The arrangement of a common cryptographic system is shown in the Figure 1 below shown.

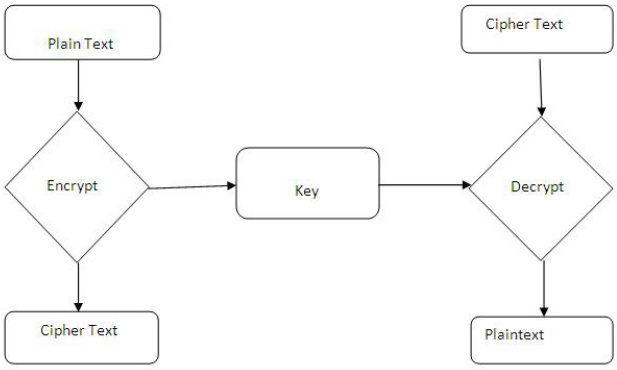

Figure 1. Structure of cryptographic system.

1.1 Elliptic_Curves

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987) and Victor Miller (Miller 1986) independently proposed the public key cryptosystems using elliptic curve. The ECC is a realistic, secured technology to be implemented in constrained applications. Generating curves to work as cryptographic curves must go through numerous algorithms and procedures so as to create a reliable cryptographic curve.

The ECC has been commercially accepted and adopted by many standardizing bodies such as American National Standards Institute and Institute of Electrical and Electronics Engineers, International Organization for Standardization and National Institute of Standards and Technology (NIST). ANSI in their standard provides the needed algorithms to generate an elliptic curve and generating Elliptic Curve Digital Signature (ECDSA) signatures[6].

The image encryption algorithm is used to transmit the image securely. So that no illicit user can capable to decrypt the data. So the Public Key encryption approaches are protected only when the authenticaton of the public-key is to be confident. The Elliptic curve cryptography performed with various numerical operations are used to develop a range of Elliptic Curve Cryptographic (ECC) schemes including key exchange and encryption and the digital signature.

2. Proposed Method of Implementation

Providing security to images are most significant. The methods used that includes a novel level of authentication and identification to applications devoid of their risks and challenges. The existing techniques to afford security of image with image encryption remain unsatisfactory facing to the rising security requirements. The proposed protocol is implemented that provides secured authentication to integrate the image with Elliptic Curve Cryptography to provide security.

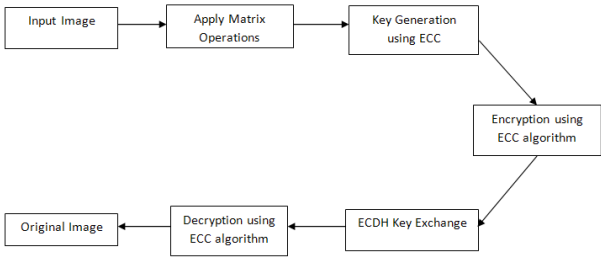

Figure 2. Block diagram of proposed method.

2.1 Steps involved in Proposed Method are:

- Matrix operations.
- Image Encryption using ECC algorithm.
- ECDH Key Exchange.
- Decryption using ECC algorithm.

2.1.1 Matrix-Operations

Step 1: Input the Image.
Step 2: Symbolize the Image in the form of RGB matrix(Depends on the pixel size of image).
Step 3: Now Divide RGB matrix into three individual R and G and B matrices.
Step 4: And then perform the transformations operations on individual matrices.

2.1.2 Imge-Encryption using ECC

Step 1: Obtain the domain Parameters of EC, D = (*q, FR, a, b, G, n, h*).
Step 2: Plot the chosen Elliptic curve.
Step 3: Achieve key pair by means of ECC domain parameters.

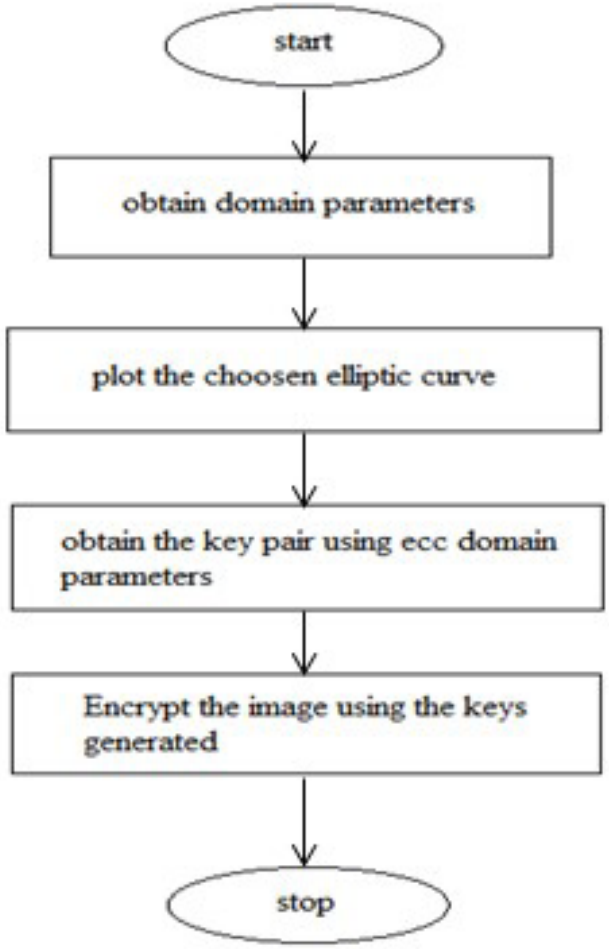

Figure 3. Encrypting image using ECC.

Step 4: Encrypt the Image with the help of the keys generated.

Encryption steps:
PmI=aPm // a: pixel value of the image from image grid // Pm: random point on EC
PB=nB * G
// G is the base point of EC
// nB is the private key
CipherText={kG,PmI+k*PB}

For mapping the image on the Elliptic Curve we used the following steps:
Assume the following elliptic curve $Y^2 \bmod p = (x^3 + ax + b) \bmod p$
The elliptic curve y^2 Mod 47 = X^3 +43 x+ 30 Mod 47 is employed in this work. i.e. by choosing a=43, b=30 and p=47.

Points on EC are:

Table 1. Generation of points

(0,1),(1,3)	(2,11),(3,31)	(4,26),(5,2)
(6,8,) (7,7)	(8,5),9,8)	(10,22),(11,10)
(12,21),(13,18)	(14,7),(15,37)	(16,28)

2.1.3 ECDH Key Exchange

Step 1: Sender(S) sends by using his public key to the Receiver and keeps its private key secret.
Step 2: Receiver(R) sends its public key to Sender and keeps its private key secret.
Step 3: Sender(S) finds the Key by means of Sender's private key and receiver's public key.
Step 4: Receiver calculates its Key by means of Sender's private key and Sender's public key.
In the key exchange process, we followed the below steps:
Step 1: At first Sender(S) sends the Image by way of the key calculated at Sender side.
Step 2: Receiver(R) verifies the Key sent by the Sender with the key calculated at Receiver side.
Step 3: If both the keys are matched, Receiver can decrypt the Image with the key pair generated.

2.1.4 Image-Decryption using ECC

Decryption steps for B:
Step 1: Decrypt the Image using Key pair. Decryption process includes the following operations.
Let kG be the first point and PmI + k*PB is the second point .

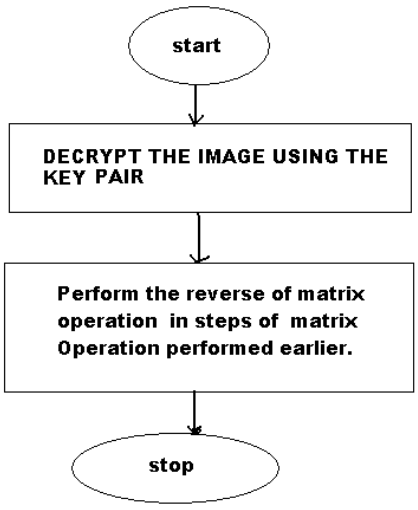

Figure 4. Image decryption using ECC.

nBkG = nB * first point;
Calculate PmI = PmI + kPB- nBkG;
An attacker required to compute *k* given *G* and *kG*, which is assumed hard.
Compute the values of Pm from the values of PmI by using discrete logarithm.
Step 2: Perform Reverse of the Matrix operations in steps of **Matrix operations** performed earlier.

3. Results

By choosing the select button we can select the image that go for encryption process.

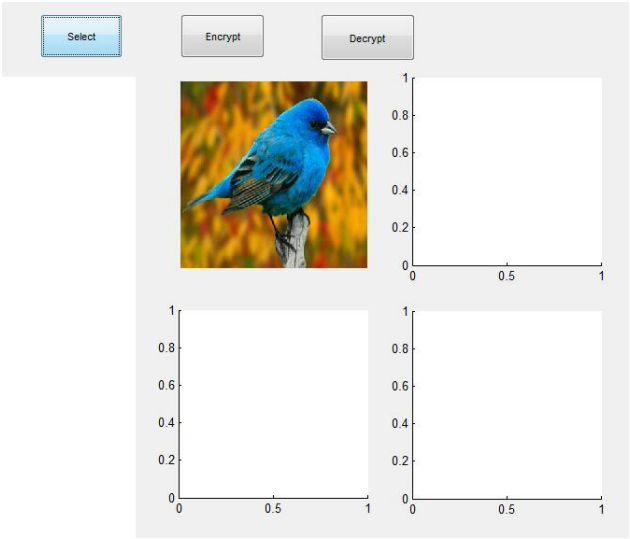

Figure 5. Image selected.

In the Figure 6 shown below, key is generated using the given curve choosen below and by selecting Encrption option, the image was encypted.

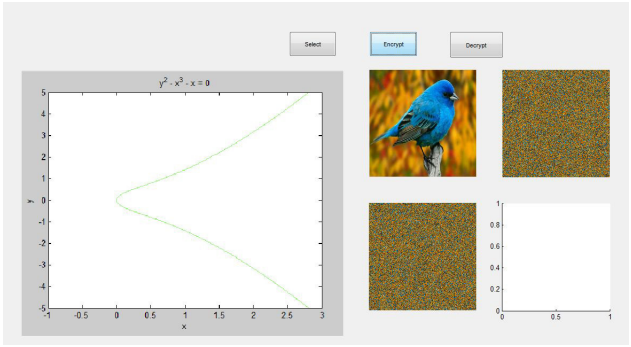

Figure 6. Key is generated and the Image is encrypted.

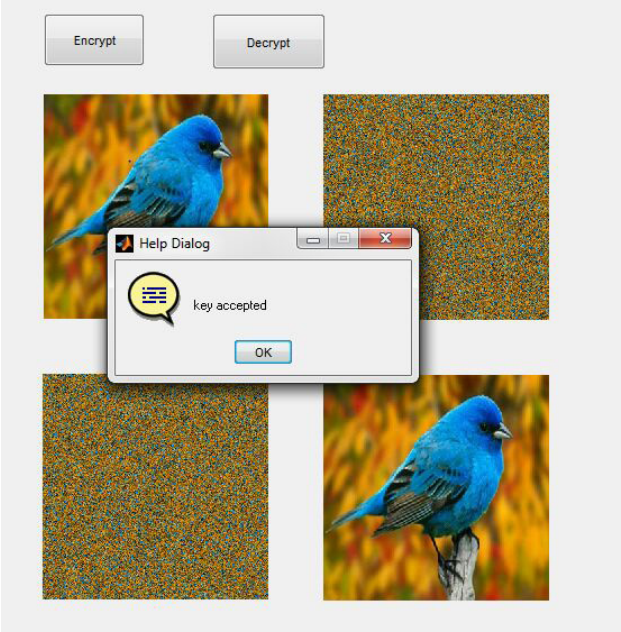

Figure7. Key is verified.

To authenticate the image key verification using ECDH is performed.

4. Conclusion

Elliptic Curve Cryptography is an advanced algorithm which provides more security. The other Public Key Cryptographic methods are does not provide that much security when compared to ECC[7]. This is because in cryptography there may be a chance of code breaking after making cryptanalysis but in this system keys are generated using elliptic curves which are difficult to exploit. The feature of ECC which include the benefits of higher-strength per-bit higher speeds with lower power consumption and bandwidth savings and storage efficiencies. In this paper we implemented a technique on BMP images. In this work, image security is provided by implementing ECC Algorithm. Transformations[8] are performed on the original image matrix and the transformed image is further encrypted with the help of a key sequence which is generated from the elliptic Curve (The intensity of each pixel is transformed into the elliptic curve and encrypted using ECC). The encrypted image is decrypted by using the key generated from the chosen elliptic curve and then we perform the reverse transformations on the matrix obtained. We are implementing authentication and verification using ECDH key exchange.

This technique can be further enhanced by making this method compatible to encrypt multimedia data or any other data which has to be transmitted securely. As mobile usage is being wide these days[9], we can even use this technique with mobile environment for safe transmission of images.

5. References

1. Kolhekar M, Jadhav A. Implementation of Elliptic Curve Cryptography on text and image. Enterprise Computing and Business System International Journal l. 2011 Jul; 1(2):1–13.
2. Yen JC, Guo JI. A new chaotic key-based design for image encryption and decryption. IEEE International Conference Circuits and Systems; Geneva. 2000. p. 49–52.
3. Mitra A, Subba Rao Y V, Prasnna SRM. A new image encryption approach using combinational permutation techniques. Journal of Computer Science. 2006; 1(2):127–31.
4. Sinha A, Singh K. A technique for image encryption using digital signature. Source: Optics Communications. 2003 Apr; 218(4-6):229–34.
5. Ahirwal RR, Ahke M. Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network. International Journal of Computer Science and Information Technologies. 2013; 4(2):363–8.
6. Thangarasu N. Implementation secure authentication using Elliptic Curve Cryptography. International Journal of Innovative Research in Advanced Engineering (IJIRAE). 2014 Mar; 1(1):41–4.
7. Ozturk I, Sogukpınar I. Analysis and comparison of image encryption algorithms. Journal of Transactions on Engineering, Computing and Technology. 2004;1(2):64–7.
8. Shuihua H, Shuangyuan Y. An asymmetric image encryption based on matrix transformation. ECTI Transactions on Computer and Information Technology. 2004 Oct; 1:66–9.
9. Prabhakar M. Anna University, Chennai, India. Elliptic Curve Cryptography in securing networks by mobile authentication. IJCIS. 2013 Sep; 3(39):31–46.