An Extensive Review on Elliptic Curve Cryptography for Ciphering Images

Harsha Singh[1] , Prof. S. R. Yadav[2]

[1]PG Scholar , Mtech(CSE),[2] HOD , CSE

Millennium Institute Technology and Science, Bhopal, India

Abstract - security of data to maintain its confidentiality, proper access control, integrity and availability has been a major issue in data communication. As soon as a sensitive message was etched on a clay tablet or written on the royal walls, then it must have been foremost in the sender's mind that the information should not get intercepted and read by a rival. Codes, hence, form an important part of our history; starting from the paintings of Da Vinci and Michelangelo to the ancient Roman steganographic practices the necessity of data hiding was obvious. The use of Elliptical Curve Cryptography for ciphering color images is reliable and secures [1]. ECC has been proved to score over RSA on the basis of its strength and speed. In this paper methodologies has been reviewed which is used to encrypt image using ECC color image ciphering.

Keywords- Elliptic Curve Cryptography (ECC), ciphering, steganography, Access control, Rivest Adi Shamir (RSA).

I. INTRODUCTION

In the information age, sharing and transfer of data has increased tremendously and usually the information exchange is done using open channels which can make it vulnerable to interception. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts [1]. Steganography and cryptography are the two important tools to protect information.

Steganography is the art of hiding data in the images. Usually, the data is hidden in the least significant bits of the pixels. But, the LSB steganography is not a robust data hiding technique as it is highly susceptible to cropping, rotation, low bit reverse attack due to LSB weakness and other geometrical attacks and compression techniques. Moreover, an adversary can also erase the message by zeroing the LSB plane, as the perceptual quality if the image doesn't get affected with the least significant bits.

Data encryption is another way of protecting the data. Usually stream encryption is employed to protect the data. In stream encryption each plaintext bit is encrypted one at a time with the corresponding bit of the key stream, to give a bit of the cipher text stream.

The pseudo random key stream is generated sequentially from a random seed value using shift registers. However, Stream ciphers are highly susceptible to known-plaintext attacks.

The encrypted message is called ciphertext. The process of retrieving the plaintext from the ciphertext is called decryption. Modern cryptography, as applied in the commercial world, is concerned with a number of problems. The most important of these are:

1) Confidentiality, which is the process of keeping information private and secret so that only the intended recipient is able to understand it.
2) Authentication, which is the process of providing proof of identity of the sender to the recipient, so that the recipient can be assured that the person sending the information is who or what he or she claims to be.
3) Integrity, which is the method to ensure that information, is not tempered with during its transit or its storage on the network.
4) Non-repudiation, which is the method to ensure that information, cannot be disowned. Once the non-repudiation process is in place, the sender cannot deny being the originator of the information.

A. The Cipher System

Substitution cipher is one of the basic constituents of classical ciphers. A substitution cipher is a method of encryption by which units of plaintext are exchanged with ciphertext according to a normal system; the flats may be lone notes, in double of notes, triplets of notes, blends of the overhead, and so forward. The receiver deciphers the text by accomplishing an inverse substitution. The units of the plaintext are retained in the identical sequence as in the ciphertext, but the flats themselves are changed. The following flowchart in Figure 1.1 below shows the basic symmetrical cryptosystem structural design that is used for image cipher [7].

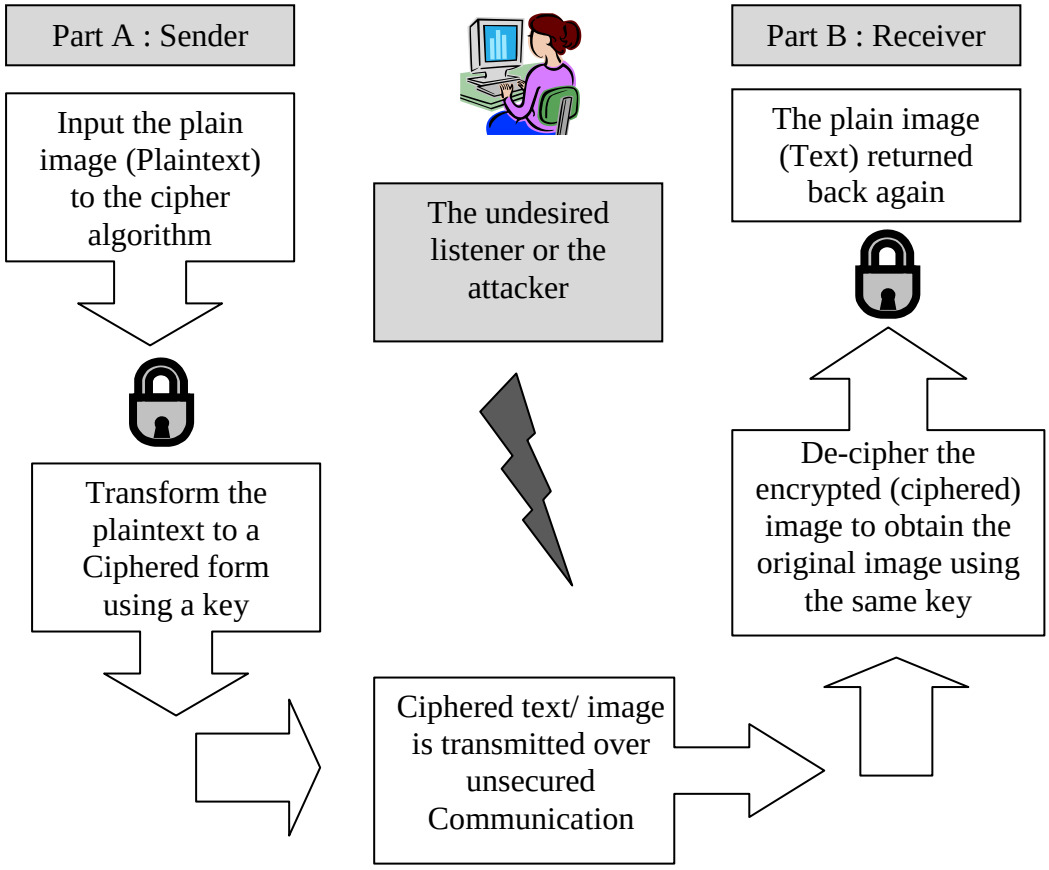

Figure 1.1 The Symmetric cipher system structure

II. ELLIPTIC CURVE CRYPTOGRAPHY

Public key cryptography systems are usually based on the assumption that a particular mathematical operation is easy to do, but difficult to undo unless you know some particular secret. This particular secret that serves as the secret key. A recent development in this field is the so-called Elliptic Curve Cryptography. Elliptic Curve Cryptography works with point on a curve. The security of this type of public key cryptography depends on the elliptic curve discrete logarithm problem. Elliptic curve cryptography was invented by Neil Koblitz in 1987 and by Victor Miller in 1986. The principles of elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or EIGamal. Although no general patent on elliptic curve cryptography appears to exist, there are several patents that may be relevant depending on the implementation . The main advantage of elliptic curve cryptography is that the keys can be much smaller. Recommended key sizes are in the order of 160 bits rather than 1024 bits for RSA.

A. Elliptic Curves:

An elliptic curve is a set of points (x, y), for which it is true that

$$y^2 = x^3 + ax + b \dots\dots\dots\dots\dots 2.1$$

Given certain chosen numbers a and b. Typically the numbers are integers (whole numbers), although in principle the system also works with real (fractional) numbers. Despite what the name suggests, the curves do not have an elliptic shape. For example, a=-4 and b = 0.67 gives the elliptic curve with equation $y = x - 4x + 0.67$.

III. RELATED WORK

N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal,[1] The growing dire need for more and more secure systems has led researchers worldwide to discover and implement newer ways of encryption. Public key cryptography techniques are gaining worldwide popularity for their ease and better strength. With the rapid developments of the communication and applications of multimedia techniques in recent years lead the researchers to focuses on the security of digital data over the internet. N. Gupta Discussed the use of Elliptical Curve Cryptography for ciphering color images. ECC has been proved to score over RSA on the basis of its strength and speed. NIST

Curves used for ciphering color image.

N. Thiranant, Y. J. Kang, T. Kim, W. Jang, S. Park and H. Lee,[2] The development of internet and new technology has been growing continuously, smartphone is now a necessary device that has great impact on users in various ways. Internet and smart devices have gained their success in various fields and have provided conveniences to all types of users. The flow of data is seen as a part of the internet and smart devices. Since a large amount of users rely on the internet for their own purposes, it then has become a big vulnerable target for attackers. a design of elliptic curve cryptography-based authentication using Quick Response Code (QR Code) is proposed. It mainly focuses on QR Code, as it is now widely used all over the world. However, the enhancement of the existing approaches is encouraged by the fast development of threats, which are presently encountered. The encryption process is included, and the proposed authentication protocol applies the concepts "Something you know" and "Something you have". Normally, people are not concerned about the threats behind the process of transmitting information over the internet, especially through QR Code. With this authentication process, users can ensure that they and their information are safe from online threats.

D. E. M. Ahmed and O. O. Khalifa,[3] With the ease of editing and perfect reproduction in digital multimedia, the protection of ownership and the prevention of unauthorized tampering of multimedia data (audio, image, video, and document) become important concerns. Steganography is one of these schemes that entails the opportunity to hide any secret information into images. Recently there are many techniques used for robust and secure image steganography, that can trade off between the capacity, payload, security, minimizing distortions of the image and high robustness. All these are challenges that need to implement a suitable technique that verify the most of these challenges. However developing a robust and secure image steganographic technique against detecting ability need to combined cryptography and steganography. The issue of secure and robust image data hiding is proposed through using (LSB) technique and Elliptic curve cryptography (ECC). The proposed scheme allow the sender to select a suitable cover and secret message that decidable to transmit through unsecure channel and then encrypt the message using (ECC) and embed it by (LSB) into selected cover.

L. Dolendro Singh and T. Debbarma,[4] There are lots of cryptosystem which provides high security but they all come with a price that is large key size which requires high computing power device. Researchers have come up with an alternative for this that provides high security with smaller key size. This alternative is the Elliptic Curve Cryptosystem. deals with the mathematics involve in the cryptosystem and an approach to work with smaller key size when the elliptic curve equation and the generator are kept secret between the users.

C. Fu, G. y. Zhao, M. Gao and H. f. Ma,[5] Chaos-based image cipher has been extensively investigated over the last two decades or so to meet the increasing demand for secure image transmission over open networks. a chaotic symmetric image cipher with permutation-diffusion architecture is presented. In the permutation stage, we introduce a novel shuffling method, which swaps each pixel in plain image with another pixel at a location chosen by chaotic Hénon map . Compared with conventional permutation schemes based on area-preserving chaotic maps, such as baker map, Arnold cat map, and standard map, the new scheme is superior in both effectiveness and efficiency. In the diffusion stage, each shuffled pixel is masked according to both key stream element and previous ciphered pixel so as to make the cryptosystem secure against differential attack. Intensive cryptanalysis is carried out and the experimental results demonstrate that the cryptosystem can withstand all kinds of known attacks, including brute-force attack, differential attack, known/chosen plain-text attack as well as various statistical attacks.

T. T. K. Hue, T. M. Hoang and S. A. Assad,[6] proposes and investigates a Chaotic Cipher Block Chaining mode (CCBC) which is to improve the security of a cryptographic algorithm and more resisting cryptanalysis. The size of both block and key are 512-bits. This approach makes the size of key greater than those of the current Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The security analysis process proves that the proposed algorithm can resist the statistical and differential attacks. It also passed the key sensitivity test. The experimental results on Field Programmable Gate Array (FPGA) show the feasibility and effectiveness of the cryptosystem and indicates the trade-off between secure/performance/efficient and architecture hardware design.

IV. PROBLEM STATEMENT

There is the possibility that someone else opens the letter or reads the electronic communication. The solution to this problem is cryptography. Cryptography enables us to store sensitive information or transmit it across insecure networks, like the Internet, so that it cannot be read by anyone else except the intended recipient. The security of data is big challenge now days there are many algorithms and techniques are proposed by researchers but still the security of information is challenging. Elliptic curve cryptography is the most popular among the modern

ciphering technique and can be the best solution for the future security.

V. PROPOSED METHODOLOGY

There are several methods of conventional cryptography, and since it is not possible to present all the methods, very important and popular methods were presented.

And to extend the technological improvements in the cryptographic techniques below are the proposed solutions can be adopted:

a. Arnold Chaotic Map

The algorithm provides a method for purpose of encrypting and decrypting the image of any size and shape. It allows the user to select an image of his choice from a specified location on the computer, external hard drive or any other hardware devices connected to the computer. The image selected by the user could be a Square image or a rectangular image of any dimension. The user is able to apply encryption to images captured via the camera and Personal pictures. The image selected should be a colour image where the pixels are represented in the RGB model. Each pixel should be represented using minimum 24 pixels. Once the keys have been entered by the user in any form, a standard chaotic map is generated. The chaotic map generated using Mathematical equations and theory is completely reversible, efficient enough to produce diffusion on the entire image pixels and the computation time is less. The chaotic map produced is then used for diffusing the image pixels. The image obtained from this chaos is completely distorted and the output is not recognizable by the end user.

b. Pixel Shifting Algorithm

which removes the deficiencies of both the advancing methods. In this method first we split the secret image into two parts and apply the sieving process with first advancing method on each image part. In second step we merge the shares obtained from first step and produce two encrypted image parts. In last step both encrypted parts are joined together to create the encrypted image. The encrypted image produced in this method has the size equal to original image. We can iterate this method several times to enhance the security.

VI. CONCLUSIONS

Many data hiding and data encryption techniques present in literature, there is still a lot of scope for improving them. Two new data encryption technique using images and traditional stream cipher concepts have been discussed. Data security is the main aim of any data hiding algorithm. Data hiding algorithm using ECC meets all the requirements such as secrecy, integrity, availability and authenticity. PKC's consist of encryption schemes, where the difficulty of finding the decryption key without knowledge of the encryption key, is based on a mathematical problem which is believed to be nearly impossible to solve in reasonable time. This way, the encryption key can be made public, and this solves the problem of exchanging keys in the traditional secret key cryptosystems.

REFERENCES

[1] N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal, "Elliptic Curve Cryptography for ciphering images," 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, 2015, pp. 1-4.

[2] N. Thiranant, Y. J. Kang, T. Kim, W. Jang, S. Park and H. Lee, "A Design of Elliptic Curve Cryptography-Based Authentication Using QR Code," 2014 IEEE 17th International Conference on Computational Science and Engineering, Chengdu, 2014, pp.

[3] D. E. M. Ahmed and O. O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography," 2014 International Conference on Computer and Communication Engineering, Kuala Lumpur, 2014, pp. 288-291.

[4] L. Dolendro Singh and T. Debbarma, "A new approach to Elliptic Curve Cryptography," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramanathapuram, 2014, pp. 78-82.

[5] C. Fu, G. y. Zhao, M. Gao and H. f. Ma, "A chaotic symmetric image cipher using a pixel-swapping based permutation," 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013), Xi'an, 2013, pp. 1-6.

[6] T. T. K. Hue, T. M. Hoang and S. A. Assad, "Design and implementation of a Chaotic Cipher block chaining mode for image encryption," 2013 International Conference on Advanced Technologies for Communications (ATC 2013), Ho Chi Minh City, 2013, pp. 185-190.

[7] Panigrahy S. K., Acharya B., Jena D., "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", 1st International Conference on Advances in Computing, Chikhli, India, pp. 21-22, February 2008.

[8] Padma Bh, D.Chandravathi, P.prapoorna Roja: "Encoding and decoding of a message in the implementation of Elliptic Curve Cryptography using Koblitz Method". International Journal on Computer Science and Engineering (IJCSE) Vol. 02, No. 05, 2010, 1904-1907.

[9] Kamlesh Gupta1, Sanjay Silakari, "ECC over RSA for Asymmetric Encryption: A Review"