An Extensive Review on Elliptic Curve Cryptography for Ciphering Images

Tarendra Rahadave[1], Dr. Vikas Gupta[2]

[1]*M-Tech Research Scolar,* [2]*Research Guide*

Department of Electronics & Communication Engg. TIT, Bhopal

Abstract: - Cryptology is the branch of science that deals with the hiding of information and protection of important information from the intruder. It is used to make sure the secrecy about the transmitted data over an unsecure channel and prevent eavesdropping and data tampering. Many cryptography schemes areused for securing data, some of the authors has been used different cryptography schemes as the shared key cryptography, while some others use Elliptic Curve Cryptography for ciphering color image. So by using different cryptography schemes the performance of the system can be enhanced. In this review the comparative analysis through the literature review has been presented in order to improve the system performance of Image Cryptography for ciphering (encoding) color image.

Keywords—Encryption, Elliptic Curve Cryptography (ECC).

I. INTRODUCTION

Elliptical Curve Cryptography was introduced by Neal Koblitz and Victor S. Miller. It makes use of the structure of elliptic curves over finite fields. ECC has the advantage of smaller key size over the earlier public key cryptosystems in turn demanding lesser storage requirements [3]. Theoretically the strength of elliptical curves can be attributed to the ease of finding a resultant point on the curve by multiplying a given point by a random number but deciphering the number even after knowing the given and resultant point is a herculean task [5].

Cryptography is based on hard mathematical problems like prime number factorization, Elliptic curve discrete logarithm problem and discrete logarithm problem. The idea behind these problems is the computation can be easily done in one direction, but it is very difficult in the opposite direction. It is not difficult to find the result of multiplying two numbers, but it is extremely challenging to find prime factors of a number. Thus, cryptography is concerned with the design and the analysis of mathematical techniques which can offer secure communications in the presence of malicious adversaries. It is an area which is concerned with the transformation of data for security reasons.

Before moving further, these are a number of terms which are commonly associated with cryptography:

Plaintext: The message which is transmitted to the recipient.

Encryption: The procedure of changing the content of a message in a way that it conceals the real message.

Ciphertext: The output which is produced after encrypting the plaintext.

Decryption: The reverse function of encryption. It is the process of retrieving the plaintext from the ciphertext.

Types of Cryptography

Cryptographic systems can be divided into two types, namely Symmetric and Asymmetric cryptography. Both are used to protect the communication privacy between the entities to avoid eavesdropping and alteration. The next analysis study provides a discussion on both types of cryptography and discuses their advantages and disadvantages.

Symmetric Cryptography

Symmetric cryptography (shared key) is a cryptosystem which provides the ability to secure exchange of messages between two ends. At the initial stage, the entities intend to communicate agree on a key.

Asymmetric-Key Cryptography

Asymmetric-key cryptography, known as the public-key cryptography (PKC), The idea of public-key cryptography is defining two different keys; one key (private key) is used to encrypt the plaintext and the other key (public key) to decrypt it. To send a message to a node, e.g. Bob; Bob‟s public key is used by Alice to encrypt the message. The cipher can only be decrypted using Bob‟s private key. The basic protocol between the two parties, i.e. Alice and Bob, is depicted in Fig. 1.1, in which EKpup is Bob‟s public key, and Kpr is Bob‟s private key.

Public-key schemes require the communicating parties to exchange keying material in an authenticated way. Despite the fact that the PKC has achieved all the security services, it still has some disadvantages as compared to the symmetric cryptography:

- Asymmetric encryption process uses a complicated mathematics compared to symmetric cryptography.
- The asymmetric cryptography algorithms are much computationally demanding than the symmetric key algorithms.

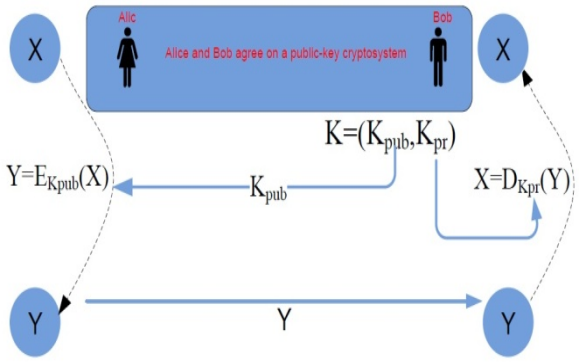

Fig. 1.1 Public Key Encryption Protocol.

Even when the Public Key (PK) is properly analyzed, it is still very slow as compared to the best known private key schemes. A hybrid cryptography scheme was introduced; it is a mixture of the PK and the symmetric cryptography, and is used in some applications. The hybrid cryptosystem uses the PKC to agree on the shared key, and then it uses the symmetric cryptography to encrypt and decrypt the messages. The public key cryptosystem algorithms can be categorized into three different groups, such as:

Algorithms based on the Discrete Logarithm Problem (DLP)[1]

The method to solve a given instance of the DLP is dependent on the size of the parameters, and each time, the parameter size increases the difficulty of solving the problem. Given positive numbers a and b, find positive integer k such that b = a.k mod p, i.e. Diffie and Hellman and digital signature Algorithm (DSA).

Algorithms based on the Integer Factorization Problem (IFP)[3]

As for the integer factorization problem, its hardness is important for the security of the RSA public-key encryption and signature schemes. The problem of hardness resulted from the difficulty of finding the prime factorization of a given positive integer n,.

Algorithms based on Elliptic Curve Discrete Logarithm Problem (ECDLP)

The challenging part of this problem is to find the positive integer k given two points P and Q on an elliptic curve over a finite field, such that Q = k * P, i.e. the Elliptic Curve Digital signature algorithm (ECDSA).

The shared key cryptography, the public key cryptography is rather slow. However, the public-key cryptography can be used with 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 not required.

Elliptic curve cryptography[1]

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985 independently proposed the public key cryptosystems using elliptic curve. Since then, many researchers have spent years studying the strength of ECC and improving techniques for its implementation. The Elliptic curve cryptosystem (ECC) provides a smaller and faster public key cryptosystem. In addition, the ECC is also a realistic and secured technology to be implemented in constrained applications, such as the RFID.

The ECC has been commercially accepted, and adopted by many standardizing bodies such as American National Standards Institute ANSI, Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO) 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. It provides step-by-step examples to generate and verify ECDSA to differentiate key sizes. Study will give an overall overview of the standard efforts.

Elliptic curves defined over finite fields which provide a group structure used to analysis the cryptographic schemes. Scalar point multiplication is a major building block of all elliptic curve cryptosystems, an operation of the form $k \cdot P$, where k is a positive integer and P is a point on the elliptic curve. Calculating $k \cdot P$ gives the result of adding the point P to itself for the exact k-1 times, which results in another point Q on the elliptic curve. The inverse operation, i.e. to recover k when the points P and Q = $k \cdot P$ are given is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP). No sub exponential-time algorithm has been known to solve the ECDLP in a properly selected elliptic curve group. The Elliptic curve cryptography offers two major benefits over the RSA; it has more security per bit and a suitable key size for hardware and modern communication. Accordingly, this results in smaller public key certificates, lower power requirements and smaller hardware processors.

To increase the security and make use of the biometric features by generating private keys and producing Elliptic Curve domain parameters, this study combined the elliptic curve and biometric features to harden the seed that will be used to generate the curve against the cryptanalysis. The

intended system uses iris signature as an input data to help generating the intended Elliptic Curve parameters. The generated parameters will be used in the cryptography process such as Elliptic Curve Digital Signature Algorithm (ECDSA).

Integrity can be resolved using a suitable mode of operation with a symmetric cipher. Authentication in the symmetric cryptography can be achieved only if there are two entities sharing the same key. Authentication is to ensure the sender identity, where the assumed that only two entities has the same key, so the receiver will be sure that the sender entity is the one who is sharing the same key with.

Assume that A and B are using the Internet as their communications channel as it is depicted in Fig.1.2. EVE could try to read the traffic from A to B; therefore, learning A‟s credit card information, or could attempt to masquerade as either A or B in the transaction. Another example, consider a situation where Alice is sending an email message to Bob over the same medium (Internet). Eve could attempt to read the message or even modify it or send a message to Bob as if it was sent from Alice.

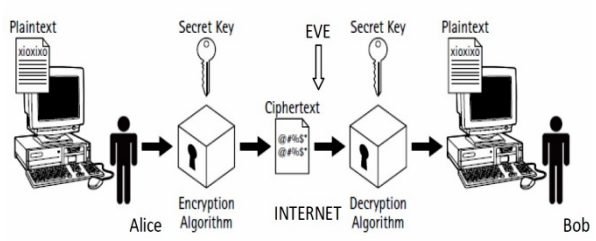

Fig.1.2 Communication over insecure line.

II. LITERATURE SURVEY

SR. NO.	TITLE	AUTHORS	YEAR	METHODOLOGY
1	Design and implementation stegocrypto based on elgamal elliptic curve	Litasari , B. Rahadjo	2017	stegocrypto uses ElGamal's elliptic curve for the coding process and utilizes noise as a steganographic medium. The elliptic curve used in this study has 2026 pairs of points
2	A novel image encryption scheme based on different block sizes for grayscale and color images	O. Reyad, M. A. Mofaddel, W. M. Abd-Elhafiez and M. Fathy	2017	two image encryption schemes are proposed for grayscale and color images.
3	Cryptographic turbo code for image transmission over mobile networks	V. Sawant , A. Bhise,	2016	Cryptographic Turbo Code (CTC) is a modification of the existing TC to provide encryption and error correction as a single entity. Encryption of data is achieved by the proposed Elliptic Curve Cryptographic Interleaver (ECCI) of CTC.
4	Chaos-based cryptography for cloud computing,	P. Tobin, L. Tobin, M. Mc Keever and J. Blackledge	2016	The alleged presence of backdoors in common encryption ciphers and a system for addressing this problem is discussed.
5	Elliptic Curve Cryptography for ciphering images	Gupta, N, Kundu, V,Kurra, N,Sharma, S,Pal, B	2015	In this research they have discussed the use of Elliptical Curve Cryptography for ciphering colour images. They have used NIST Curves for ciphering colour image.
6	Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)	Sowmya, S, Sathyanarayana, S.V.	2014	In this research, cyclic elliptic curve of the form y2 = x3 + ax + b, a, b ∈GF(p) with order M is considered and key Sequences are derived from random sequence of cyclic elliptic Curve points. A pseudorandom sequence generator based on chaotic function

				and Elliptic Curve arithmetic over GF (p) is proposed here.
7	Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network	Baheti, A, Singh, L, Khan, A.U.	2014	This investigation introduces an efficient symmetric encryption scheme based on a cyclic elliptic curve and chaotic system that can overcome these disadvantages. The cipher encrypts 256-bit of plain image to 256-bit of cipher image within eight 32-bit registers.
8	A binary grouping approach for image encryption based on elliptic curves over prime group field	Soleymani, A, Nordin, M.J, Md Ali, Z, Golafshan, L.	2013	On Elliptic Curve Cryptography (ECC), this is a public-key cryptosystem for encoding data and forwarding over unsecure networks.
9	A Novel Cryptosystem Based on Iris Key Generation	Xiangqian Wu, Ning Qi, Kuanquan Wang, Zhang, D.	2008	This investigation proposes a novel biometric cryptosystem based on the most accurate biometric feature - iris.

Litasari and B. Rahadjo [1] Well-known techniques for securing data are cryptography and steganography. Cryptography is an information security technique that turns information into another random and incomprehensible form, while steganography secures data by hiding information in storage media such as text, images, sound and video. In this research will be merged both security techniques, namely Stegocrypto. This stegocrypto uses ElGamal's elliptic curve for the coding process and utilizes noise as a steganographic medium. The elliptic curve used in this study has 2026 pairs of points. While the input of this system is an ASCII character, so input should be represented first before being processed. The process of inserting cipher with noise is done without using a marker. In this study, the stegocrypto system was successfully implemented. The system successfully encrypts and decrypts the input message. Decryption is done by reading all received stego-noise and will be read as cipher text when it is an elliptic group element. Then from the test is also obtained the influence of message length and k variables to the time required for the process of encryption and decryption.

O. Reyad, M. A. Mofaddel, W. M. Abd-Elhafiez and M. Fathy,[2] In this investigation, two image encryption schemes are proposed for grayscale and color images. The two encryption schemes are based on dividing each image into blocks of different sizes. In the first scheme, the two dimension (2D) input image is divided into various blocks of size N × N. Each plainimage block is transformed into a one dimensional (1D) array using the Zigzag pattern mode. Then, the exclusive or (XOR) logical operation is used to encrypt each block with the analogous secret key. In the second scheme, after the transformation process, the first block of each image is encrypted by the corresponding secret key. Then, before the next block is encrypted, it is XORed with the first encrypted block to become the next input to the encrypting routine and so on. This feedback mechanism depends on the cipher block chaining (CBC) mode of operation which considers the heart of some ciphers because it is highly nonlinear. In the case of color images, the color component is separated into blocks with the same size and different secret keys. The used secret key sequences are generated from elliptic curves (EC) over a binary finite field F2™. Finally, the experimental results are carried out and security analysis of the ciphered images are demonstrated that the two proposed schemes had a better performance in terms of security, sensitivity and robustness.

V. Sawant and A. Bhise,[3] Mobile communication has become an essential part of our daily life for accessing and sharing data over internet in addition to voice communication. Mobile communication channel is an open network and hence maintaining the confidentiality and reliability of the data has always been an area of concern. Reliability of data against channel noise can be ensured by various error correcting codes. Turbo Code (TC) is an excellent channel encoder with near Shannon limit error correction performance. However, TC does not guarantee the security of the transmitted image against intruders on the wireless channel. Proposed Cryptographic Turbo Code (CTC) is a modification of the existing TC to provide encryption and error correction as a single entity. Encryption of data is achieved by the proposed Elliptic Curve Cryptographic Interleaver (ECCI) of CTC. The ECCI is an asymmetric private key interleaver which shuffles the input bit sequence based on the Elliptic Curve (EC) arithmetic and a private key. Shuffling the bits also reduces its correlation and improves the error correction performance of the code. The CTC ensures the secrecy of the shared private keys over an insecure wireless channel by Elliptic Curve Diffie-Hellman Key Exchange

(ECDHKE). This makes the CTC robust against cryptographic attacks. The qualitative and quantitative performance analysis of the proposed code is evaluated to validate its effectiveness for image transmission over a mobile network in contrast to other state-of-art methods. Simulation results illustrate a similar coding gain, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) for images retrieved by the proposed CTC, encrypted TC and TC for authorized users. Additionally, it ensures security of the data from unauthorized users as compared to TC. Investigation results also depict the strength of CTC against Brute Force, known plaintext, chosen plaintext and cipher text attacks.

P. Tobin, L. Tobin, M. Mc Keever and J. Blackledge, [4] Cloud computing and poor security issues have quadrupled over the last six years. The alleged presence of backdoors in common encryption ciphers and a system for addressing this problem, is discussed. In 2007, two Microsoft employees gave a presentation “On the Possibility of a backdoor in the NIST SP800-90 Dual Elliptic Curve Pseudo Random Number Generators” which was linked in 2013 by the New York Times with notes leaked by Edward Snowden. This confirmed backdoors were placed, allegedly, in a number of encryption systems by the National Security Agency. If true, it creates an urgent need for personalising the encryption process by generating locally, an unlimited number of the unbreakable one-time pad ciphers. Hybrid random binary sequences generated from chaotic oscillators initialised by natural noise, were exported to an online Javascript application. The online software uses a von Neumann deskewing algorithm to improve the cryptographic strength of the encryptor and also provides an initial statistical p-test for randomness. Encoding the Lenna image by XORing it with the new cipher provided another quick test to observe if any patterns are in the encoded image, otherwise the cipher is subjected to the NIST suite of statistical tests. All designs were simulated in Orcad PSpice© V16.5 prior to prototype construction.

Gupta, N.et.al. [5] 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. In this research they have 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. In this investigation they have used NIST Curves for ciphering color image.

Sowmya, S. and Sathyanarayana, S.V., [6] Until recently, Cryptography has been of interest primarily to the military and diplomatic communities. But the dawning of the information age has revealed an urgent need for cryptography in the private sector too. Cryptography is the study of techniques for ensuring the secrecy and authentication of the information. In this research, cyclic elliptic curve of the form $y2 = x3 + ax + b$, $a, b \in GF(p)$ with order M is considered and key Sequences are derived from random sequence of cyclic elliptic Curve points. Elliptic Curve is a cubic equation in two variables, x and y, with coefficients from a field satisfying certain conditions. For cryptographic applications the coefficients are chosen from finite fields. A pseudorandom sequence generator based on chaotic function and Elliptic Curve arithmetic over GF(p) is proposed here. The randomness properties of this sequence have been tested using various techniques like, auto-correlation distribution, crosscorrelation distribution and first return map. It is observed that the sequence generated satisfies the required randomness properties. These sequences find applications in Stream Cipher Systems. An additive Stream Cipher system is designed

using this sequence as the key sequence to encrypt images. Results of image encryption and decryption for a medical image is discussed and analyzed in this research work. The security analysis of the proposed system is also discussed.

Baheti, A.; et.al [7] as multimedia applications are used increasingly, security becomes an important issue of security of images. The combination of chaotic theory and cryptography forms an important field of information security. In the past decade, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic maps have been proposed. But, most of them delay the system performance, security, and suffer from the small key space problem. This investigation introduces an efficient symmetric encryption scheme based on a cyclic elliptic curve and chaotic system that can overcome these disadvantages. The cipher encrypts 256-bit of plain image to 256-bit of cipher image within eight 32-bit registers. The scheme generates pseudorandom bit sequences for round keys based on a piecewise nonlinear chaotic map. Then, the generated sequences are mixed with the key sequences derived from the cyclic elliptic curve points. The proposed algorithm has good encryption effect, large key space, high sensitivity to small change in secret keys and fast compared to other competitive algorithms.

Soleymani, A.; et.al. [8] This is a investigation on Elliptic Curve Cryptography (ECC), which is a public-key cryptosystem for encoding data and forwarding over unsecure networks. The technical description and benefits of ECC are stated and contrasted with other cryptosystems.

This is then followed by a proposal for a new image cryptosystem, which is based on the binary value of pixels and grouping bits. A simple application is executed to show how the ECC can be used to convert, group, map and encrypt an image. Finally, an analysis is carried out to ascertain the strength of the encrypted image to withstand statistical and brute force attacks.

Xiangqian Wu; et.al. [9] Biometric cryptography is a technique using biometric features to encrypt data, which can improve the security of the encrypted data and overcome the shortcomings of the traditional cryptography. This investigation proposes a novel biometric cryptosystem based on the most accurate biometric feature - iris. In encryption phase, a quantified 256-dimension textural feature vector is firstly extracted from the preprocessed iris image using a set of 2-D Gabor filters. At the same time, an error-correct-code (ECC) is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using Hash function. Some general encryption algorithms use this cipher key to encrypt the secret information. In decryption phase, a feature vector extracted from the input iris is firstly corrected using the ECC. Then it is translated to the cipher key using the same Hash function. Finally, the corresponding general decryption algorithms use the key to decrypt the information. Experimental results demonstrate the feasibility of the proposed system.

III. PROBLEM & PROPOSED WORK

Elliptic Curve Cryptography had been used for doing asymmetric cryptography in base research work [1].Recommended RSA key size for most applications. But the security level maybe improved further. For further enhancement of the security in images one should increase the levels of encryption for ciphering the color images so that the images would be secured with mixing of pixel intensities by interchanging their indexes in a specified way for encryption.

IV. CONCLUSION

As e-governance is the present trend of administration and management, encryption of data has become a necessity. Image encryption has widespread applications including Government, military, financial institution, hospitals and private business. The growing for more and more secure systems has led researchers worldwide to discover and analysis 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. This review discussed about different types of use of Elliptical Curve Cryptography for ciphering color images. The work will be done to achieve benefits and security parameters.

REFERENCES

[1]. Litasari and B. Rahadjo, "Design and implementation stegocrypto based on elgamal elliptic curve," 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, 2017, pp. 95-99.

[2]. O. Reyad, M. A. Mofaddel, W. M. Abd-Elhafiez and M. Fathy, "A novel image encryption scheme based on different block sizes for grayscale and color images," 2017 12th International Conference on Computer Engineering and Systems (ICCES), Cairo, 2017, pp. 455-461.

[3]. V. Sawant and A. Bhise, "Cryptographic turbo code for image transmission over mobile networks," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016, pp. 844-850.

[4]. P. Tobin, L. Tobin, M. Mc Keever and J. Blackledge, "Chaos-based cryptography for cloud computing," 2016 27th Irish Signals and Systems Conference (ISSC), Londonderry, 2016, pp. 1-6.

[5]. Gupta, N.; Kundu, V.; Kurra, N.; Sharma, S.; Pal, B., "Elliptic Curve Cryptography for ciphering images," in Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on., pp.1-4, 24-25 Jan. 2015.

[6]. Sowmya, S.; Sathyanarayana, S.V., "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)," in Contemporary Computing and Informatics (IC3I), 2014 International Conference on , pp.1345-1350, 27-29 Nov. 2014.

[7]. Baheti, A.; Singh, L.; Khan, A.U., "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network," in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on , pp.664-668, 7-9 April 2014.

[8]. Soleymani, A.; Nordin, M.J.; Md Ali, Z.; Golafshan, L., "A binary grouping approach for image encryption based on elliptic curves over prime group field," in Communications (MICC), 2013 IEEE Malaysia International Conference on., pp.373-378, 26-28 Nov. 2013.

[9]. Xiangqian Wu; Ning Qi; Kuanquan Wang; Zhang, D., "A Novel Cryptosystem Based on Iris Key Generation," in Natural Computation, 2008. ICNC '08. Fourth International Conference on , vol.4, pp.53-56, 18-20 Oct. 2008.

[10]. Zhang Yun-Peng; Liu Wei; Cao Shui-ping; ZhaiZheng-jun; NieXuan; Dai Wei-di, "Digital image encryption algorithm based on chaos and improved DES," in Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, pp.474-479, 11-14 Oct. 2009.