International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 06, Issue: 03 (May-June, 2020)

Effective Secret Communication in Preventing Cybercrime Using Advanced Elliptic Curve with Multiple Image Encryption

Vikas Vishwakarma, Shital Gupta, Rahul Tiwari
Computer Science Department, SORT People's University, Bhopal
[1]vickyvishwakarma9300@gmail.com,[2]email4sgupta@gmail.com, [3]rahultiwari3189@gmail.com

***Abstract**: To improve encryption efficiency and facilitate the secure transmission of multiple digital images, by defining the pure image element and mixed image element, this paper presents a new multiple-image encryption with advance elliptic curve algorithm based on the mixed image element and permutation, which can simultaneously encrypt any number of images. Firstly, segment the original images into pure image elements; secondly, we can encrypt our original image many types as per need for our security once encryption is done, we decrypt our image for get original message. The comparison with two similar algorithms is made. Experimental results and algorithm analyses show that the proposed algorithm is very simple and efficient, which is suitable for practical image encryption.*

Keywords: Cyber Security, Cyber Space, Cyber Crime, Cryptography, Elliptic Curve.

I. INTRODUCTION

Cryptography deals with hiding information in such a way that allows information to be sent in a secure form so that only person able to retrieve hided information is the intended recipient. In present times, cryptography is considered as a branch of both mathematics and computer science, and is affiliated closely with information theory, information security and engineering technology. Use of cryptography is growing in various applications where information security is mainly concerned. Examples include the ATM transaction security, computer passwords security, and electronic commerce security, which all depend on robust cryptographic algorithms [1].

In recent years there has been significant interest in reversible data hiding, and also in particular, reversible data hiding in encrypted images (RDH-EI). This means that additional data can be embedded into a previously encrypted image with no knowledge of the originalimage content. According to the held keys, legal receivers can get the embedded data or an image very similar to the original one or, both the embedded data and an image exactly as the original one. In this paper, we propose and evaluate a RDH-EI framework. Firstly, we propose a multi-level encryption (MLE) scheme using both Josephus traversal based multi-granularencryption and a stream cipher. To reduce the quantity of side information required to embed into images together with additional data, we also present a block histogram modification (BHM) approach with self-hidden peakpixels to perform reversible data embedding and a location map marking scheme to perform histogram contraction and recovery. The experimentalresults demonstrate that, in comparison with other similar methods, the proposedframework achieves improvements in terms of the embedding payload, the decrypted imagequality and the accuracy of image restoration. Encryption and decryption of plain text shown in fig 1

Figure: 1 Encryption and decryption process

In Paper [3] Resource constrained sensing devices are being used widely to build and deploy self-organizing wireless sensor networks for a variety of critical applications such as smart cities, smart health, precision agriculture and industrial control systems. Many such devices sense the deployed environment and generate a variety of data and send them to the server for analysis as data streams. A Data Stream Manager (DSM) at the server collects the data streams (often called big data) to perform real time analysis and decision-making for these critical applications. A malicious adversary may access or tamper with the data in transit. One of the challenging tasks in such applications is to assure the trustworthiness of the collected data so that any decisions are made on the processing of correct data. Assuring high data trustworthiness requires that the system satisfies two key security properties: confidentiality and integrity. To ensure the confidentiality of collected data, we need to prevent sensitive information from reaching the wrong people by ensuring that the right people are getting it. Sensed data are always associated with different sensitivity levels based on the sensitivity of emerging applications or the sensed data types or the

sensing devices. For example, a temperature in a precision agriculture application may not be as sensitive as monitored data in smart health. Providing multilevel data confidentiality along with data integrity for big sensing data streams in the context of near real time analytics is a challenging problem. In this paper, we propose a Selective Encryption (SEEN) method to secure big sensing data streams that satisfies the desired multiple levels of confidentiality and data integrity. Our method is based on two key concepts: common shared keys that are initialized and updated by DSM without requiring retransmission and a seamless key refreshment process without interrupting the data stream encryption/decryption. Theoretical analyses and experimental results of our SEEN method show that it can significantly improve the efficiency and buffer usage at DSM without compromising the confidentiality and integrity of the data streams.botnet. Distributed computing worldview permits theinternet cyber space.

II. SECURITY REQUIREMENTS IN CYBER SPACE

The goal of security services in cyber space is to protect the information and resources from attacks and misbehavior. The security requirements in WSN include:

Confidentiality: Confidentiality is hiding the information from unauthorized access. In many applications, nodes communicate highly sensitive data. A sensor network should not leak sensor reading to neighboringnetworks. Simple method to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers 'possess, hence achieving confidentiality. As public key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods. For symmetric key approach the key distribution mechanism should be extremely robust.

Authentication: Authentication ensures the reliability of the message by identifying its origin. In a WSN, the issue of authentication should address the following requirements: [1] communicating node is the one that it claims to be (ii) the receiver should verify that the received packets have undeniably come from the actual sensor node**.** For Authentication to be achieved the two parties should share a secret key to compute message authentication code (MAC) of all communicated data. The receiver will verify the authentication of the received message by using the MAC key.

Integrity: Integrity is preventing the information from unauthorized modification. Data authentication can provide data integrity also.

Availability: Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks**.**

III. CRYPTOGRAPHY

Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. But as the sensor nodes are limited in their computational and memory capabilities, the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them. Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. But as the sensor nodes are limited in their computational and memory capabilities, the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them.

A. Symmetric Cryptography: Symmetric encryption (also called as secret-key cryptography) uses a single secret key for both encryption and decryption as shown in Figure 2.

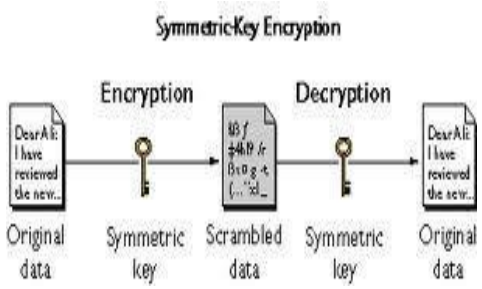

Figure 2: Symmetric -Key Cryptography

This key has to be kept secret in the network, which can be quite hard in the exposedenvironment where WSNs are usedto achieve the security requirements, several researchers have focused on evaluating crypto graphical algorithms in WSNs and proposing energy efficient ciphers. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES, 3DES etc [4].

B. Asymmetric Cryptography

Asymmetric encryption (also called public-keycryptography) uses two related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed. A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. Likewise, a message that is encrypted by using the

private key can only be decrypted by using the matching public key. Examples are RSA, ECC etc.

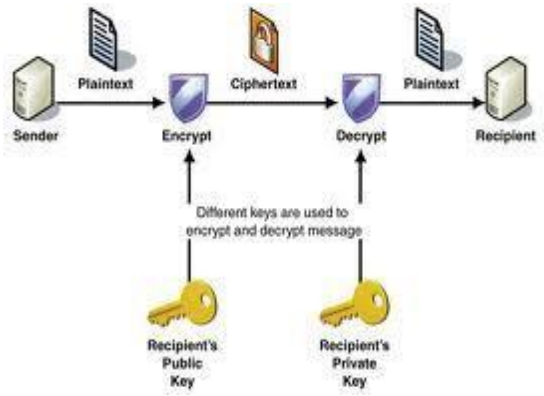

Figure 3: Asymmetric Key Cryptography

IV. PROPOSED WORK

In this Paper RSA and proposed Multiples image encryption technique has been discussed this algorithm followed by several step.

A. RSA Algorithm

A method to implement a public key cryptosystem whose security is based on the difficulty of factoring large prime numbers was proposed in [05]. *RSA* stands for Ron Rivest, Adi Shamir and Leonard Adelman, who first publicly described the algorithm in 1977. Through this technique it is possible to encrypt data and createdigital signatures. It was so successful that today *RSA*public key algorithm is themost widely used in theworld.

Key generation:

1. *Choose two distinct prime numbers, p and q.*
2. *Compute modulus n = pq*
3. *Compute phi, φ= (p - 1) (q - 1) where φ is Euler's Totient Function.*
4. *Select public exponent e such that 1 < e < φ and gcd(e, φ) = 1*
5. *Compute private exponent d = e -1mod φ*
6. *Public key is {n, e}, private key is d*

Encryption: c = me (mod n).
Decryption: m = cd (mod n).

B. ECC (Elliptic curve cryptography) [06]

This algorithm is mainly depending on the algebraic structure of elliptic curves. The difficulty in problem is the size of the elliptic curve. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements—i.e., that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key—e.g., a 256bit ECC public key should provide comparable security to a 3072bit RSA public key(see #Key sizes).For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation: y2=x3+ax+b, Compared to RSA,ECC has small key size, low memory usage etc. Hence it has attracted attention as a security solution for wireless networks [07].

C. Proposed Multiple Image Encryption Technique

The technique of multiple encryptions in the proposed scheme is based on well-established data encryption algorithm called Elliptic Curve Cryptography (ECC). Performing the process of encryption several times enhance the security by minimizing key size by splitting it in every phase. It enhances security because of performing the same operation multiple times with different encryption key at every step. Due to repetitive application of encryption algorithm increases time complexity but at the same time splitting the main key into part key reduces time complexity to some extent. An example of multiple encryption technique is given below. Example of Multiple Encryption Technique: In cryptography, we would expect that by encrypting a plaintext twice with some block cipher, either with the same key or by using two different keys, the resultant encryption to be stronger in almost all circumstances. By using this process, we would expect to achieve more security. For example, a plaintext ‚cryptography' is passes through Caesar cipher encryption, *N=3* times at which multiple encryption gives substantial improvements in security. Let original data/ plaintext be cryptography [8]

Algorithm: C = ((P + 3) + 3) + 3 …….. + 3) (N Times)

Table: 1 process of multiple encryptions

C	R	Y	P	T	O	G	R	A	P	H	Y	Plain Text
F	U	B	S	X	R	J	U	D	S	K	B	Cipher Cycle#1
I	Y	E	V	A	U	M	Y	G	V	N	E	Cipher Cycle#2
L	B	H	Z	D	Y	P	B	J	Z	Q	H	Cipher Cycle#3

This process of multiple encryptions can be performed with different encryption keys at each phase and process can be repeated number of times as desired.

D. Key Exchange between User A and B

Elliptic curve cryptographic key exchange can be done in the following way. First a large integer q is chosen randomly, which is either a prime number p or an integer of the form $2^m$and elliptic curve parameters a and b for the elliptic curve equation. This defines the elliptic group of points $E_p(a,b)$. Next, pick a base point $G=(x_1,y_1)$ in $E_p(a,b)$whose order is very large order value n. The order n of a point G on an elliptic curve is the smallest positive integer n such that nG=O. $E_p(a,b)$ and G are parameters of the cryptosystem known to all parties.

A key exchange between the intended users can be accomplished as shown in the figure 2.

1. Alice selects an integer n_A less than n. This is Alice's private key. A then generates a public key $P_A = n_A \times G$; where the public key is a point in $E_p(a,b)$.
2. Bob similarly selects a private key $n_B$and computes a public key P_B.
3. Alice generates the secret key $k = n_A \times P_B$ .Bob generates the secret key $k = n_B \times P_A$.

These two calculations in step 3 produce the same result because

$$n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A$$

To break this scheme, an attacker would need to be able to compute K for given G and kG, which is assumed hard.

Message Encryption:

Message m is considered as a point Pm with coordinates (x, y) in the elliptic curve Pm. The point Pmis encrypted as a ciphertext Cm and subsequently decrypted.

To encrypt and send a message *Pm* to Bob, Alice chooses a random positive integer *k* and produces the ciphertext *Cm*consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Steps of Encryption
Step 1 Input Message
Step 2 Encode Using ECC
Step 3 Input Multiple Images
Step 4 Encrypted Images
Step 5: Again, Encrypt the Image Using ECC
Step 6: Final Encrypted Image

This algorithm work on multiple image encryption technique using ECC. This method follows the five steps in which first we provide the input image or message. The input message is encoded with ECC. Then this message or image work as input message the again this message is encrypted as by following the reverse encryption, we decrypt the image. Figure 4 shows the details.

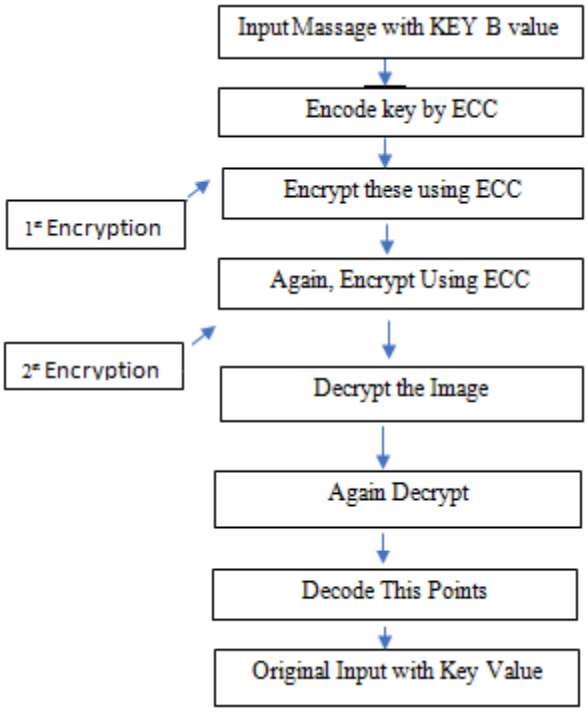

Figure: 4 proposed work model

V. SIMULATION TOOL AND RESULT ANALYSIS

A. Simulation Tool:

The Performance analysis of MATLAB version (R2013a) i.e. used for this thesis Implementation of information mining provides processor optimized libraries for quick execution and computation and performed on input cancer dataset. It uses its JIT (just in time) compilation technology to supply execution speeds that rival traditional programming languages. It may also additional advantage of multi core and digital computer computers, MATLAB give several multi-threaded algebra and numerical operate. These functions automatically execute on multiple process thread during a single MATLAB, to execute quicker on multicore computers. During this thesis, all increased efficient information retrieve results were performed in MATLAB (R2013a). MATLAB is that the high-level language and interactive environment utilized by a lot of engineers and scientists worldwide. It lets the explore and visualize concepts and collaborate across totally different disciplines with signal and image process, communication and computation of results. MATLAB provides tools to accumulate, analyze, and visualize information, modify you to induce insight into your information during a division of the time it'd take exploitation spreadsheets or traditional programming languages. It may also document and share the results

through plots and reports or as printed MATLAB code. MATLAB (matrix laboratory) could be a multi paradigm numerical computing scenario and fourth generation programming language. It's developed by math work; MATLAB permits matrix strategy, plotting of operates and knowledge, implementation of rule, construction of user interfaces with programs. MATLAB is meant in the main for mathematical computing; an optional tool box uses the MuPAD symbolic engine, permitting access to symbolic computing capabilities. It's simulating on mat research lab (R2013a) for this work we use Intel 1.4 GHz Machine and OS window7, window-xp etc.

Table 2 result analysis

S.N.	No of Char or Bits	Enc. Time	Dec. Time
1	10	1.2728	0.2019
2	50	2.6465	0.5248
3	100	4.5452	1.2264
4	150	6.228	1.6546
5	200	8.7701	2.5052
6	300	12.4489	3.6054
7	400	14.8965	4.6824
8	500	18.4845	5.7656
9	800	30.5746	9.6813
10	1000	36.501	10.7001

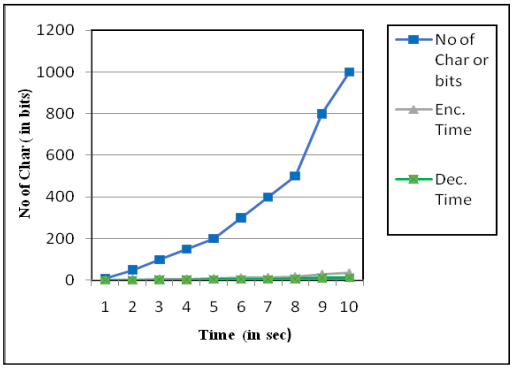

Figure 5: Result graph of encryption and decryption time

B. Result Analysis:

As they can see in figure 4, in Multiple ECC the plaintext with is encrypted to get two ciphertext points and again these points are encrypted to get ciphertext points and the process is repeated in reverse to get the original plaintext message. Hence encrypting the plaintext with image again and again with same or different key multiple times makes an encryption technique a multiple encryption technique. This increases the security as well as complexity and makes it more and more difficult for an attacker to break the ciphertext. In our final result we have calculate the time with help of MATLAB tools. The result table 2 shown below. Result Show in graph is found out encryption and decryption time less as compare existing method. It also called our proposed method best for images bits or char encryption and decryption.

VI. CONCULSION

Cyber security is very essential for every computer user Cyber bullying means harming or harassing via information technology networks in a repeated manner. That could be done via text messages or images, personal remarks posted online, hate speeches etc. cyber bullies may also disclose victims' personal data (Like real name, address) on website. In this paper we have discussed the Advance ECC algorithm in which we have calculated encryption and decryption time which is better than previous ECC based algorithm. RSA has been in public key systems for over two decades, but ECC offers an alternative. ECC is exciting because of the potential to provide similar levels of security compared to RSA but with significantly reduced key sizes. ECC presumably offers faster processing, and lower demands on memory and bandwidth, which are critical in the space of mobile solutions. Currently, the research on the threshold cryptography develops fast. However, the threshold cryptography technologies based on ECC deserve great attention.

VII. ACKNOWLEDGMENTS

This research was supported/partially supported by my guide prof Rahul Tiwari Assistant Professor SORT (Computer Science Department) Peoples University. We thank my friend from SORT people's university who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

I thank Mr. Ankit Temurnikar, PhD Research Scholar (Computer Science Department), Bhagwant University for assistance with cybercrime, cyber security technique, using algorithm and methodology also guidance, inspiration to the right path in every step of its building, for this motivation.

I would also like to show our gratitude to my family sharing their pearls of wisdom with us during the course of this research. Although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

[1]. Vishal Kumar, Ratnesh Kumar, Mashud A. Barbhuiya and Monjul Saikia, "Multiple Encryption using ECC and Its Time Complexity Analysis" IJERT,2016.

[2]. Zhaoxia Yin1,2 &Andrew Abel 3 &Jin Tang2 &Xinpeng Zhang1 &Bin Luo2 "Reversible data hiding in encrypted images basedon multi-level encryption and blockhistogram modification"springer,2016

[3]. Deepak Puthal, Xindong Wu, Surya Nepal, Rajiv Ranjan and Jinjun Chen " SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams"IEEE,2017

[4]. Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques "AJER, 2014.

[5]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2):120-126, 1978.

[6]. Kristin Lauter, Microsoft Corporation , —The Advantages Of Elliptic Curve Cryptography For Wireless Security IEEE Wireless Communications ,Vol 3,pp 22-25,February 2004.

[7]. Dona Maria Mani, Nishamol P H, "A Comparison between RSA and ECC in Wireless Sensor Networks", International Journal of Engineering Research & Technology, Volume 2 Issue 3, March-2013.