ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Security Enhancement Approach For Data Transfer Using Elliptic Curve Cryptography And Image Steganography

Sudipta Sahana[1], MadhusreeMajumdar[2], Shiladitya Bose[3], AnayGhoshal[4]

Asst. Prof, Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India[1]

B. Tech, Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India[2]

B. Tech, Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India[3]

B. Tech, Department of Computer Science and Engineering, JIS College of Engineering, Kalyani, India[4]

Abstract: Securing data is a challenging issue in today's era. Keeping it in mind we have proposed a new technique which is the combination of Elliptic Cryptography and image Steganography enhanced with a new secure feature for generation of a new, robust security system. Encryption is used to transmit data securely in open public networks. Each type of data has its own added features. With the evolution of internet, security of digital images has become more and more important. Therefore different techniques should be used to protect confidential image data from unauthorized access. In this paper we have encrypted data using matrix and elliptic curves and used the concept of Steganography by hiding the generated points of the encrypted data in an image. Basically we have proposed a hybrid model using public key based Elliptical Curve Cryptography (ECC) and image Steganography which provide more security than a Single ECC or Steganography methods alone. Encryption and Decryption process are given in details with example. The comparative study of proposed scheme and the existing scheme is made. Our proposed algorithm is aimed at better encryption for all types of data and the output stego images reveal that our proposed method is robust. The main objective is to help users from different community to transfer crucial information securely who are using public network for communication.

Keywords: Elliptic Curve Cryptography, Image Stegnography, Co-*ordinate geometry*, Prime Matrix, Mask Matrix.

I. INTRODUCTION

Exchanging information over internet has become an inevitable part of our daily life. But maintaining privacy is highly doubtful. So, encryption is the only way out to transform our information into human inaccessible format. Cryptography is the technique where security engineering meets mathematics. Encryption uses mathematical schemes and algorithms to scramble the content of a message.[1] Likewise a decryption algorithm takes an encrypted and restores it to its original form for using one or multiple keys. Generally cryptographic keys are broadly classified into Private & Public keys. Public encryption is also known as asymmetric- key encryption and in lieu of private encryption is known as symmetric key encryption[2][3]. The private key is known only to your computer, while the public key is given by your computer to any computer that needs communication with it in a secured manner. In this paper, secured data transfer with the help of cryptography with Boolean algebra & key concept is highly emphasized.

Cryptosystems based on Elliptic Curves are one of the latest developments in Public-Key Cryptography. Proposed a decade after RSA algorithm, they received increased commercial acceptance and were included in important security standards. Nowadays, they are among the most attractive candidates in new developments of cryptographic schemes both in hardware and software. Thanks to the unique properties of elliptic curves, the cryptosystems based on them achieve a desired security level with significantly smaller keys than the more conventional schemes (for instance, a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key). Another fascinating application of elliptic curves is in the so called identity-based cryptosystems: in 1984, A. Shamir posed a question whether there a public-key encryption scheme may be built based on users' identities (personal ID, e-mail etc.) as public keys, as opposed to classical public-key cryptography where public keys should be authorized. The first fully functional such system was proposed only in 2001, built in essential way on elliptic curves.

Steganography is the way of hiding data in an image to make secure data transfer. One of the most popular steganography technique is LSB or least significant bit insertion[9][10]. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel. To correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.
In section 2 we have done a brief literature survey of existing technique followed by our proposed method in section 3. Example has been discussed in section 4. Section 5 is all about the result analysis and in section 6 we conclude our paper.

II. RELATED WORK

To highlight the performance of the compared algorithms, this section discusses the techniques obtained from other resources.

P.Marwaha et al. [4] proposed the Cryptography and steganography are the most extensively used techniques. Both these techniques provide some security of data neither of them individually is secure enough for sharing information over an un secure communication channel and are unguarded to intruder attacks.

MonalisaDey et al. [5] have proposed encryption as a critical security measure for protecting data privacy. The entire process is done on binary data to cover all kinds of data in the field of Computer Science thus ensuring data security irrespective of what information is being exchanged.

Darrel Hankerson et al. concluded that Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [6].His book has a strong focus on efficient methods for finite field arithmetic (Chapter 2) and elliptic curve arithmetic (Chapter 3). Next, Chapter 4 surveys the known attacks on the ECDLP, and describes the generation and validation of domain parameters and key pairs, and selected elliptic curve protocols for digital signature, public-key encryption and key establishment

In [7], G. Zhu et al. have attemted to encrypt an image by scrambling pixels and then adding a watermark to scrambled image. This paper introduced a new approach for image encryption using elliptic curve.

A. Nag et.al. proposed the embedding process [8] to ensure hiding of data under the transformation (DWT and IDWT) of cover image and to obtain privacy by using Huffman encoding. Image steganography is the art of hiding information into a cover image. This paper presents a novel technique for Image steganography based on DWT.

III. PROPOSED METHOD

In this section along with key generation algorithm we have proposed our encryption & decryption algorithm which is mainly implemented by matrix. In the algorithm from step1 to step6 we define encryption, from step7 to step 10 define stegnography.

A. Encryption Algorithm

Step1. Take the message to be encrypted from the sender.
Step2.Convert it to its 7bits binary form using the ASCII code of the message.
Step3.Convert the binary form of each word of the message into n x 7 binary matrix where n is a number of letters in each word of the message.
Step4.To get the compressed decimal matrix of size n x 1 , we will multiply the n x 7 matrix with the masked matrix of size 7 x 1.
Step5.We will get n values of 'x' and to get the corresponding 'y' values we will use the formula

$$y\text{^}2=x(i)\text{^}3+j$$

Where, i = 1 to n (and n is the no. of rows in the resultant matrix)
j is the variable which will keep on incrementing every time we get a y for a particular x value. The initial value of j = 1.
Step6. Using the formula we will get (x, y) points.
Step7.Algorithm for plotting the values of x, y:
Step7.1: Get the values of x and y and truncate the decimal values of y as well.
Step7.2: Create a matrix consisting of the decimal values of y.
Step7.3: Now find the x, y coordinates in the image.
Step7.4: inverse the bit values of the image (i.e.: if bit value=01 then make it 10) on the particular coordinates of (x, y). That will produce the stego image as well.
Step8.We will generate a prime matrix of size n x7 and using the 'x' values we will generate an equation which will resemble the decimal matrix.
Step9. Public Keys: The generated equation from the step7, prime matrix, will be send to the receiver.
Step10.Private key: the original image, the stego image, the matrix containing numbers after decimal point of the values of 'Y' and our formula (mentioned above).

B. Decryption Algorithm

Step1.The receiver will get the x and y values after comparing two images and finally get the values of y with the help of the matrix containing the values of y(after decimal points).
Step2.The required matrix will be generated using the 'x' values and the prime matrix which is public.
Step3.We will multiply the 'x' values with the prime elements and will check the result of the co-efficient with the generated public equation
Step4. In this way the receiver will generate the required matrix which will contain the binary form of the ASCII codes of the encrypted message.

IV. EXAMPLE AND DISCUSSION

Now, with the example we will show the working policy of algorithms mentioned above.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

A. Encryption Process

Word to be encrypted: JIS

LETTER	ASCII VALUE	BINARY FORM
J	74	1001010
I	73	1001001
S	83	1010011

Now the 3 X 7 matrix of the following word is:

1	0	0	1	0	1	0
1	0	0	1	0	0	1
1	0	1	0	0	1	1

Now we are going to use a masked matrix of 7 x 1 and the product of the two matrixes will give a resultant matrix of 3 x 1.

Masked matrix :

1
1
1
1
1
1
1

Hence the resultant matrix is:

1 + 0 + 0 + 1 + 0 + 1 + 0	=	**3**
1 + 0 + 0 + 1 + 0 + 0 + 1		**3**
1 + 0 + 1 + 0 + 0 + 1 + 1		**4**

So we get x1=3, x2=3, x3=4

To get the y component values we will use an elliptic curve formula.

y^2 = x(i)^3 + j (Private Key)

Where, i = 1 to n (and n is the no. of rows in the resultant matrix)
j is the variable which will keep on incrementing every time we get a y for a particular x value. The initial value of j = 1.
So, using the formula we get the points as (3, 5.3), (3, 5.4), (4, 8.2)

We will truncate the decimal values of y and store them in a matrix (which will be a private key indeed). Hence the points will be (3, 5), (3, 5), (4, 8). Then after we inverse the bit value of the image with respect to the coordinates as well.

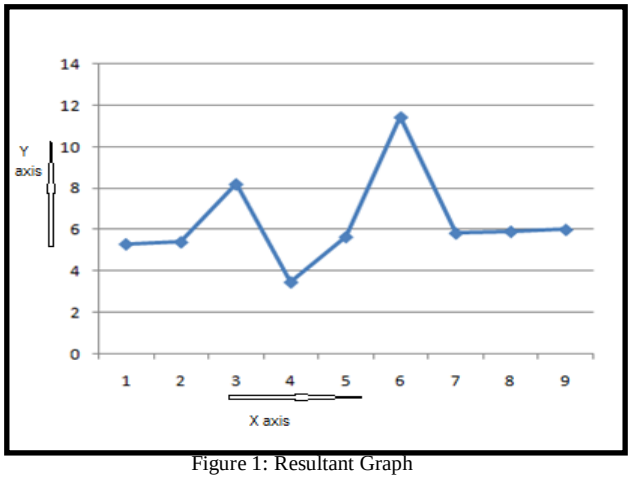

Figure 1: Resultant Graph

Public keys:

1) A n x 7 which contains the prime numbers from 1(where n is the number of the rows).
2)An equation which will be generated using the x values of the encrypted message and the matrix containing the prime numbers

2	3	5	7	11	13	17
19	23	29	31	37	41	43
47	53	59	61	67	71	73

Matrix containing the prime numbers (public)

Using the x values of the encrypted and the matrix containing the prime numbers we generate aequation:
251 x^7 + 236 x^5 + 114 x^4 + 323 x^2 + 421 x
This equation along with the matrix using the prime number will be send to the receiver and it will be public.

B. Decryption process:

The receiver will get the x and y values after comparing two images and obviously with the help of the matrix that contains the decimal values of y and using the equation send by the sender, will generate the required matrix which will contain the binary form of the ASCII codes of the encrypted message.

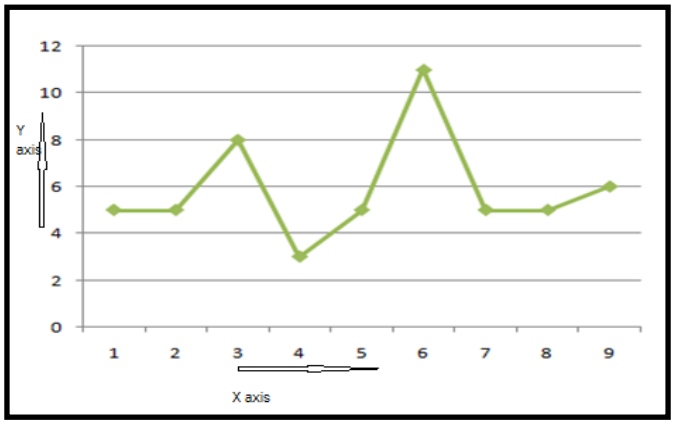

Figure 2:After applying Stegnography

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Original image

Original image+ hidden data

So the receiver gets the x values which are x1=3,x2=3,x3=4 from the graph.

Now the procedures to generate the required matrix are:

1. We will check the power of x and its coefficient. So x^7 will represent the first column of the resultant matrix as the binary form is of 7 bits. We will check whether we have to take all the x values all less to generate the coefficient of x^7.

So, 3*2+3*9+4*47=251 which is the coefficient of x^7 send by the sender. We have taken every x value to generate the coefficient so the first column of the resultant will have all 1's.

2. Similarly we see that x^6 is not present in the equation. So the second column will have all 0's. x^5 has coefficient 236 and we find that only the product of x3 with the corresponding value 59 will generate the coefficient 236. So in 3rd column x1=0,x2=0 and x1=1.

In this way we generate all the columns and get the resultant matrix as:

1	0	0	1	0	1	0
1	0	0	1	0	0	1
1	0	1	0	0	1	1

So the first row correspond to the binary of form 'J'
The second row correspond to the binary form 'I'
The 3rd row correspond to the binary form 'S'
So we get the encrypted message 'JIS'.

V. RESULT ANALYSIS

The proposed model introduced approach which is a combination of cryptography and Steganography. The goal of this technique is to put the unauthorized person in a difficult position to determine the presence of information. The dual security approach makes the information more secure .In our works we introduce [11]Elliptic Cryptography which is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields .In this Crypto method we required small key than the other Cryptography method.With our proposed approach anyone can send the data securely in public network. In this work we generate elliptic curve using matrix which is totally a new method and level of security is very high than the other approach based on this topic. To enhance the security and robustness of data transfer we apply another level of data hiding method which is Stegnography. Stegnography may be apply in various way like text, video, image. This time we use image Stegnography. Today network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding

VI. CONCLUSION

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that secrecy is *not* the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied! In fact, *time* is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys. Our proposed model is the combination of elliptic curve cryptography and image steganography. Hence it is much more secure and much more efficient to put the unauthorized person in a difficult position in the context of accessing the secure data.In fact, the plain image is divided into blocks: data matrix. The proposed cryptosystem uses a different key for mapping and encryption process and the possibility of known plaintext attack is highly reduced as the key used changes with every block and it is generated randomly using transformation algorithm based ECC.

ACKNOWLEDGMENT

We are highly indebted to our mentor Mr. Sudipta Sahana for his guidance and constant supervision as well as for providing us necessary information regarding the project. We would like to express our humble gratitude and thanks to the authors of the publications we have taken as a reference. A special thanks to our parents for their lovely support. It would not have been possible without the help of those individuals. Our sincere thanks to all of them.

REFERENCES

[1] M. M Amin, M. Salleh, S .Ibrahim, M.R.K atmin, and M.Z.I.Shamsuddin, Information Hiding using Steganography, National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003 IEEE.

[2] S Ushll , G A SathishKumal, K Boopathybagan,A Secure Triple Level Encryption Method Using Cryptography and Steganography, 20 II International Conference on Computer Science and Network Technology, 978-1-4577-1587-7/111$26.00 ©20111EEE, December 24-26, 2011

[3] . Zhang and S. Wang, Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Process.Lett., vol.12, no.I, pp. 67-70, Jan.

[4] Ipsitasahoo ,seminar report submitted in partial fulfilment of the requirements
http://www.facweb.iitkgp.ernet.in/~isg/ICTSEMINAR/R

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

EPORT-Ipsita.pdf

[5] MonalisaDey, Dhirendra Prasad Yadav, Sanik Kumar Mahata, AnupamMondal, Sudipta Sahana, "An Improved Approach of Cryptography using Triangulation and MSB Iteration Technique"Special Issue of International Journal of Computer Applications (0975 – 8887) International Conference on Computing, Communication and Sensor Network (CCSN) 2012

[6] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Guide to elliptic curve cryptography, springer.

[7] G. Zhu, W. Wang, X. Zhang, and M. Wang, "Digital image encryption algorithm based on pixels," IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), 2010, pp.769-772.

[8] A. Nag, S. Biswas, D. Sarkar, P. P.Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6),pp. 497-610,2011.

[9] S. M. MasudKarim, Md. SaifurRahman, Md. Ismail Hossain, A New Approach for LSB Based Image Steganographyusing Secret Key987-161284-908-9/11/$26.00 2011 IEEE

[10] Ahaiwe J. Document Security within Institutions Using Image Steganography Technique, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[11] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Guide to elliptic curve cryptography, springer

BIOGRAPHIES

Sudipta Sahana is an assistant professor of a renowned engineering college of West Bengal. For more than 4 years, he has worked in this region. He has passed his M.Tech degree in Software Engineering and B.Tech Degree in Information Technology from West Bengal University of Technology with a great CGPA/DGPA on 2010 and 2012 respectively. He is recently working in Ph.D. in the domain of "Cloud Computing". He has published many research paper in network security domain. He is a member of the Computer Science Teachers Association (CSTA), and also a member of International Association of Computer Science and Information Technology (IACSIT).

Madhusree Majumdar is a final year student of a renowned engineering college of West Bengal. She is currently pursuing B.Tech in computer science and engineering. The interesting world of technology always makes allurement to her. She wants to research in the domain of computer science, especially on network security.

Shiladitya Bose, a final year student of jis college of engineering, West Bengal, India. His stream of pursuit is Computer science and engineering. He is interested in the colorful domain of digital technology. Mathematics is one of his subject of passion. The immense desire to work on this domain has convinced him to take the initiative to work on a research paper on elliptic curve cryptography and steganography. He wants to do further work on cryptography and steganography, big data.

Anay Ghoshal is a final year student of a renowned engineering college of West Bengal. His stream of pursuit is Computer science. He is keen interested in the domain of network security. The immense desire to work on this domain has convinced him to take the initiative to publish a research paper on elliptic curve cryptography and steganography. He wants to do further research on networking, machine learning.