https://dx.doi.org/10.24001/ijaems.3.5.7 ISSN: 2454-1311

A New Approach of Cryptographic Technique Using Simple ECC & ECF

Neha Saini[1], Kirti Bhatia[2]

[1]M. Tech (Student), SKITM, Ladrawan,Haryana, India
[2]HOD of CSE department, SKITM, Ladrawan, Haryana, India

Abstract— *Cryptography is the technique in which usually a file is converted into unreadable format by using public key and private key system called as public key cryptosystem. Then as per the user requirement that file is send to another user for secure data transmission. In this paper we purposed an image based cryptography that Elliptic Curve Function (ECF) techniques and pseudo random encoding technique on images to enhance the security of RFID communication. In the ECF approach, the basic idea is to replace the Elliptic Curve Function (ECF) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The ECF based technique is the most challenging one as it is difficult to differentiate between the cover object and Crypto object if few ECF bits of the cover object are replaced. In Pseudo Random technique, a random key is used as seed for the Pseudo Random Number Generator in needed in the embedding process. Both the techniques used a Crypto key while embedding messages inside the cover image. By using the key, the chance of getting attacked by the attacker is reduced.*

Keyword— Cryptography,ECC,RFID,ECF.

I. INTRODUCTION

The word cryptography is derived from the Greek words Cryptos meaning cover and grafia meaning writing [1] defining it as covered writing. In image cryptography the information is hidden exclusively in images. Cryptography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as Crypto-medium. A Crypto-key is used for hiding/encoding process to restrict detection or extraction of the embedded data.

Modern cryptography concerns itself with the following four objectives:

- Confidentiality (the information cannot be understood by anyone for whom it was unintended)
- Integrity(the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
- Non- repudiation (the create/ sender of the information cannot deny at a later stage his or her intensions in the creation or transmission of the information)
- Authentication (the sender and the receiver can confirm each other's identity and the origin of information.

II. RELATED WORKS

Encryption is a method of transforming original data, called plain text , into a format appears to be random and unreadable, which is called cipher text. Plain text is either in a form of that can be understood by a person or by a computer . Once it is transformed into a cipher text , neither human nor machine can properly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without authorized disclosure. When data is stored on a computer , it is usually protected by logical and physical access controls. When this same sensitive information is sent over a network, it can no longer take these controls for granted and the information is in a much more vulnerable state.The algorithms, the set of mathematical rules, dictates how enciphering and deciphering takes place . Many algorithms are publicaly known and are not the secret part of the encryption algorithms work can be kept secret from the public , but many of them are publicaly known and well understood . If the internal mechanisms of the algorithm are not a secret , then something must be . The secret piece of using a well known encryption is the key. The key can be any value that is made upof a large sequence of random bits. Is it just any random number of bits crammed together? Not really. An algorithm contains a key space, which is a range of values that can be used to construct a key. The key is made up of random values within the key space range. The larger the key space, the more available values can be used to represent different keys, and the more random the keys are, the harder it is for intruders to figure out Cryptosystem

III. LITERATURE SURVEY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer .One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

The Frequency domain the message is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against attacks. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [3].Most of the strong cryptographic systems today operate within the transform domain Transform domain techniques have an advantage over ECF techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. An information hiding system has been developed for confidentiality. However, in this chapter, we study an image file as a carrier to hide message. Therefore, the carrier will be known as cover-image, while the Crypto-object known as Crypto-image. The implementation of system will only focus on Least Significant Bit (ECF) as one of the cryptography techniques as mentioned in below

In this technique, A random key is used to choose the pixels randomly and embed the message. This will make the message bits more difficult to find and hopefully reduce the realization of patterns in the image [9]. Data can be hidden in the ECF of a particular colour plane (Red plane) of the randomly selected pixel in the RGB colour space.

IV. PROPOSED WORK AND IMPLEMENATION

We introduce the ECC to enhance the cryptographic technique for secure transfer of secret images For RFID based communication channel. In this paper we are more focusing on Identification field of the IP header to hide secret encrypted data. Identification field is used only when fragmentation occurs. At the receiver end, to reassemble the packets, identification field tells the right order for that. If fragmentation is not occurred, then identification field will always be unused, so that we can use this 16 bit field to hide secret encrypted message. To avoid fragmentation, we use MTU. Maximum transfer unit decides limit for packet size for transmission over network. Sender and receiver, both should have awareness of MTU unit. For the encryption and decryption we use Elliptic curve cryptography. Elliptic Curve Cryptography is a public key cryptography.

Elliptic curve cryptography (**ECC**) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorizational gorithms that have applications in cryptography.

Mathematical Expression For ECC The mathematical operations of ECC is defined over the elliptic curve y = x 3 + ax + b, where 4a + 27b ≠ 0. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve **A. Performance Analysis**

As a performance measure for image distortion due to hiding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to Crypto images. It is defined as:

PSNR = 10log(Cmax)2=MSE:

MSE = mean - square - error;

Which is given as?

MSE = 1/MN ((S-C) 2):

C max = 25, Where M and N are the dimensions of the image,

S is the resultant Crypto-image, and C is the cover image.

B. Implementation and Evaluation of above two techniques

We have implemented the above two techniques in MATLAB and the above mentioned algorithms with respect to image cryptography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the cryptographic system. Some parameters are as follows :

Perceptibility does embedding information distort cover medium to a visually unacceptable level.

Capacity how much information can be hidden (relative to the change in perceptibility) item.

Robustness to attacks can embedded data survive manipulation of the Crypto medium in an effort to destroy, remove, or change the embedded data.

Table: Comparison of characters of above two techniques

Sl No.	Imperceptibility	Robustness	Capacity	Tamper Resistance
Simple ECF	High*	Low	High	Low
(ECC)	Higher**	Low	High	High**

*: Indicates dependency on the used cover image

**: Indicates dependency on the used key and ECC Key

V. CONCLUSION AND FUTURE WORK

Secure data transfer by using ECC provides an efficient technique for data hiding by using RFID channel.RFID channel is a subject which can be seen in many areas. Hiding the medium itself has a strong impact on the network communication providing high level of security and a more secure system respectively. The TCP/IP suite along with the covert medium further enhances the security of the system since attackers are more concerned over the “http”. The proposed technique will avoid illegal transmission of secret communication on the web and will provide a better secure system in case of Authentication and demand less bandwidth In Security concern it has very secured algorithm.

REFERENCES

[1] **R.Anderson and F. Petitcolas, "On the limits of cryptography" IEEE Journal of Selected Areas in** Communications, Vol. 16, No. 4, May 1998

[2] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Cryptography," IEEE computer society,2003

[3] Algorithm using ECF, DCT and Image Compression on Raw Images",Technical Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004

[4] .An overview of image cryptography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa

[5] Johnson, N.F. Jajodia, S., "Exploring Cryptography: Seeing the Unseen",Computer Journal, February 1998.

[6] Detecting ECF Cryptography in Color and Gray-Scale Images" Jessica Fridrich, Miroslav Goljan, and Rui Du State University of New York, Binghamton.

[7] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett. 36 (25) (2000) 20692070.

[8] Hiding data in images by simple ECF substitution by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

[9] A Tutorial Review on Cryptography" by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology

[10] International Journal of Computer Science Engineering Technology (IJC-SET) "Modern Cryptographic technique: A Survey" by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology.