International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

IMAGE SECURITY USING ECC AND HASH FUNCTION FOR RFID CHANNEL

Mansha[1], Asst. Prof. Nehndiratta[2]
[1]M. Tech (ECE), [1,2]DPG Institute of Technology and Management, Gurgaon

ABSTRACT: 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 the RFID communication Channel. 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.
Key word: Cryptography, ECC,RFID, MATLAB, ECF

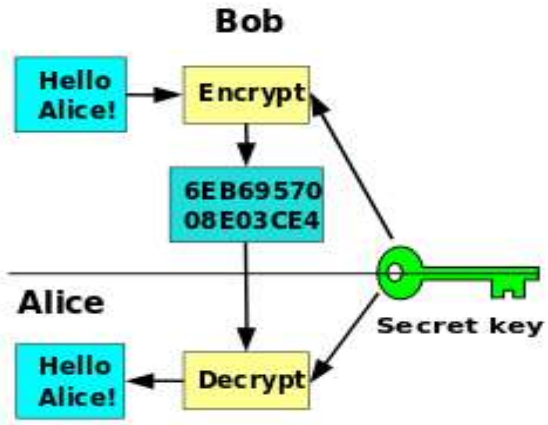
I. INTRODUCTION

A. Cryptography

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 [2].

B. Radio Frequency Identification (RFID)

RFID systems use radio frequency to identify, locate and track people, assets, and animals. Passive RFID systems are composed of three components an interrogator (reader), a passive tag, and a host computer. The tag is composed of an antenna coil and a silicon chip that includes basic modulation circuitry and non-volatile memory. The tag is energized by a time-varying electromagnetic radio frequency (RF) wave that is transmitted by the reader. This RF signal is called a carrier signal. When the RF field passes through an antenna coil, there is an AC voltage generated across the coil. This voltage is rectified to supply power to the tag.



C. Introduction A RFID over Communication Channel

RFID tag is an electronic device that holds identification data. Typically, the RFID tag is attached to items and contains a serial number, which is used to uniquely identify them. RFID technology uses radio waves to automatically identify items which have RFID tags attached to it. This technology was initially developed with the aim to manage and track items in supply chain and logistics, but nowadays it is used in many other areas e.g. medical applications, manufacturing, retail, livestock tracking and tracking exact timing in sports events.

II. LITERATURE SURVEY

Masking and Filtering is a cryptography technique which can be used on gray-scale images. Masking and filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image [5]. 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]. 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 [14]. 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 [19].

III. PROPOSED WORK

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.

A. 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.

B. Mathematical Expression For ECC

The mathematical operations of ECC is defined over the elliptic curve $y = x\ 3 + ax + b$, where $4a + 27b \neq 0$. 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.

C. 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 = 255:
Where M and N are the dimensions of the image,
S is the resultant Crypto-image, and C is the cover image.
PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is high). A high-quality Crypto image should strive for a PSNR of 40 dB, or higher

IV. 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 [13]: 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 4.1: 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.

A. Conclusion and Future Scope

Secure data transfer by using ECC provides an efficient technique for data hiding by using RFID channel. FID 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.

B. Simulation Result from MATLAB

Fig 4.1: Pic-1 has been taken for Encryption decryption

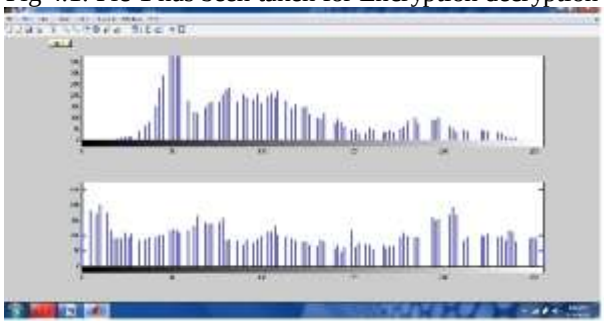


FIG 4.2: Result of fig 4.3 cryptography pic which shows increasing PSNR and reducing the distortion rate

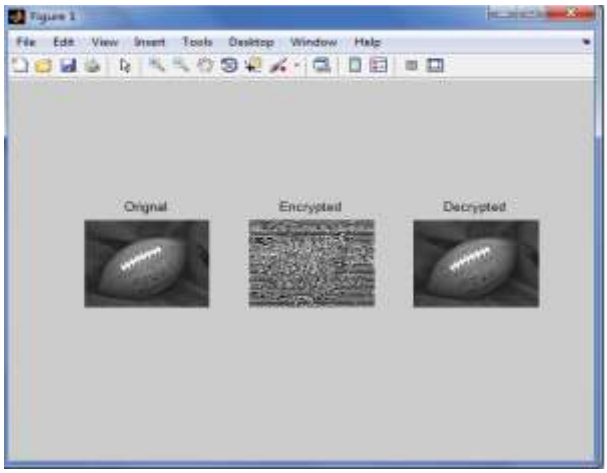
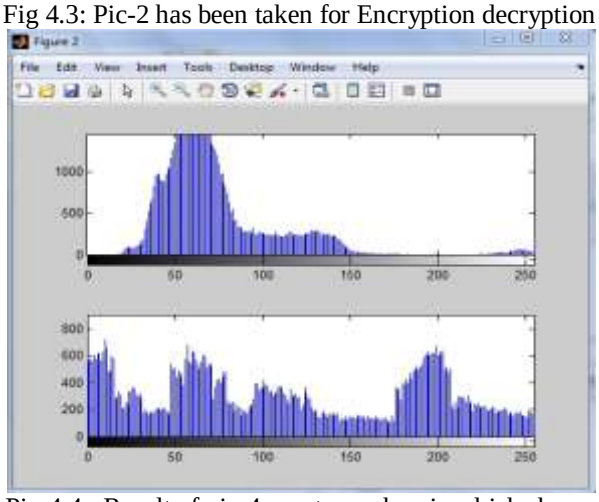


Fig 4.3: Pic-2 has been taken for Encryption decryption


Pic-4.4: Result of pic-4 cryptography pic which shows increasing PSNR and reducing the distortion rate

V. CONCLUSION AND FUTURE SCOPE

A. Conclusions

Cryptography is an effective way to hide sensitive information. In this paper we have used the ECF Technique and Pseudo-Random Encoding Technique on images to obtain secure Crypto-image. In result section this research shows that PSNR of Pseudo random encoding is higher than PSNR of ECF encoding. Our results indicate that the ECF insertion using random key is better than simple ECF insertion in case of lossless compression over RFID Communication channel. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both grayscale and color image. This paper focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

B. Future Scope

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in future. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security over RFID communication channel.

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] K B Raja, Venugopal K R and L M Patnaik, "A Secure Cryptonographic 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.

