© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Study on Combine use of Steganoghaphy and Cryptography for Data Hiding

Shailendra M. Pardeshi
Assistant Professor, Department of Information Technology, RCPIT Shirpur, India

ABSTRACT

Steganography hides the existence of message by embedding data in some other digital media like image or audio format and Cryptography converts data in to cipher text that can be in unreadable format to normal user. This paper can concentrate to make review of combine data hiding techniques useable for security of data. This paper can defines RSA algorithm for encryption and embedded encrypted data in an image using DCT based steganographic technique. The DCT based technique is better than the other techniques like LSB, Modulus arithmetic steganography.

Keywords: Data Hiding, RSA algorithm, Cryptography, Steganography.

I. INTRODUCTION

Steganography can be applied electronically by taking a message (a binary file) and some sort of cover (often a sound or image file) and combining both to obtain a "stego-object". The RS analysis is considered as one of the most famous steganalysis algorithm which has the potential to detect the hidden message by the statistic analysis of pixel values. The process of RS steganalysis uses the regular and singular groups as the considerations in order to estimate the correlation of pixels [1]. The presence of robust correlation has been witness in the adjacent pixels. But unfortunately using traditional LSB replacing steganography, the system renders the alteration in the proportion in singular and regular groups which exposes the presence of the steganography. Ultimately, it will not be so hard to decrypt the secret essage. Both the topic of steganography and visual cryptography has been considered as a distinct topic for image security. Although there are extensive researches based on combining these two approaches [2] [3], but the results are not so satisfactory with respect to RS analysis. Other conventional methods of image security has witnessed the use of digital watermarking extensively, which embeds another image inside an image, and then using it as a secret image. The use steganography in combination visual cryptography is a sturdy model and adds a lot of challenges to identifying such hidden and encrypted data. Fundamentally, one could have a secret image with confidential data which could be split up into various encrypted shares. Finally when such encrypted shares are reassembled or decrypted to redesign the genuine image it is possible for one to have an exposed image which yet consists of confidential data.

II. CONCEPT OF CRYPTOGRAPHY

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. Unfortunately, the computer security and cryptology communities have drifted apart over the last 20 years. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems. There are a number of reasons for this, such as different professional backgrounds (computer science versus mathematics) and different research funding. it is about

constructing and analysing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [4].Cryptographic systems are generically classified along three independent dimensions. Methodology for transforming plain text to cipher text. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Methodology for number of keys used. There are some standards methods which is used with cryptography such as secret key, public key, digital signature and hash function.

a) Secret Key (Symmetric): The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called as symmetric encryption.

b) Public Key: Modern Public Key Cryptography was first described publicly by Standford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their study described a two-key crypto system in which two parties could engage in a secure communication over a insecure communications channel without having to share a secret key.

c) Digital Signature: The digital signature is more like stamp or signature of the sender which is embedded together with the data and encrypts it with the private key in order to send it to the other party. In addition, the signature assures that any change made to the data that has been signed is easy to detect by the receiver.

d) Hash Function: Cryptographic hash functions are much used for digital signature and cheap constructions are highly desirable. The use of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols [5] [6]. The authentication and the integrity considered as main issues in information security, the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if it's similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side [7].

Methodology for processing plain text: A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along [8]. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

III. CONCEPT OF STEGANOGRAPHY

Steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party. In this article, I will discuss what steganography is, what purposes it serves, and will provide an example using available software. In this context, the cover medium is the file in which we will hide the hidden data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover medium). The cover medium (and, thus, the stego_medium) is typically image or audio files. In this paper, focus is on image files and will, therefore, refer to the cover image and stego_image.

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding.

IV. COMBINE STEGANOGHAPHY AND CRYPTOGRAPHY

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded [9] [10]. This combined chemistry of steganography and cryptography will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

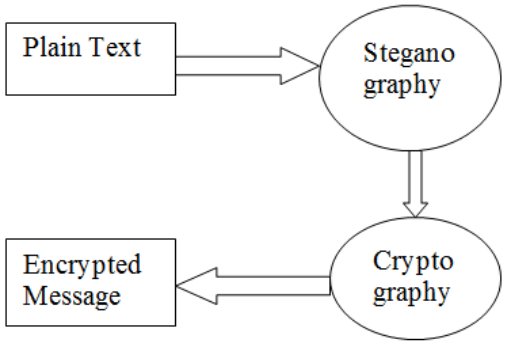

Figure 1: Combined concept of cryptography and steganography

In figure 1 both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography [11]. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types [12] [13].

A. Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

B. Secret Key steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

C. Public Key Steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier [10].

RSA is a Public key cryptography named after its inventors: Ronald Rivest, Adi Shamir and Leonard Adleman.RSA can be used for encryption as well as for authentication. An example of Alice and Bob, who want to use asymmetric RSA algorithm for secure communication. For encryption purpose, Alice would encrypt the message using Bob's Public key and send the cipher text to Bob. Upon receiving the cipher text, Bob, who is owner of corresponding private key, can then decrypt the message with his private key. For authentication purposes, Alice would encrypt (or sign) the message using her own private key [14]. Other people such as Bob can verify the authenticity of the message by using Alice's Public key, which is the only key that matches the signing private key [15].

The steps for RSA algorithm are:
1) Select two prime numbers p, q.
2) Calculate n= p × q and _(n)= (p-1)(q-1)
3) Select integer 'e' such that
gcd (_ (n),e)=1; 1<e < _(n)
4) Calculate d such that d × e=1mod(_ (n))
5) Now Public key (PU) is {e, n} and Private Key (PR) is {d, n}.
6) At sender side, message (M) to be sent is converted into cipher text (C) as follows:
C= Me mod n (1)
7) At receiver side, cipher text is converted to original message as follows:
M= Cd mod n (2)

V. CONCLUSION

The paper can discussed process of securely using steganography technique combining with visual cryptography. It can be concluded that when normal image security using steganographic and visual cryptographic technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganographic are highly optimized using genetic algorithm. The techniques are highly resilient against RS attack and optimally used for both grayscale and colored output in visual secret shares making it highly compatible for real-time applications. The future work could be towards the enhancing the algorithm using neural network for the visual cryptography, so that the system can generate highly undetectable secret shares using certain set of training data which might be automatically generated and is disposed after the task has been performed.

VI. REFERENCES

[1]. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding", I.B.M. Systems Journal, 35(3-4): pp. 313-336, 1996.

[2]. Singh Komal, K.M.; Nandi, S.; Birendra Singh, S.; ShyamSundar Singh, L.; , Stealth steganography in visual cryptography for half tone images, Computer and Communication Engineering, International Conference,

[3]. Rita Srita Rana, Dheerendra Singh, Steganography-Concealing Messages in Images Using LSB Replacement Technique with Pre-Determined Random Pixel and Segmentation of Image, International Journal of Computer Science & CommunicationVol. 1, No. 2, July-December 2010, pp. 113-116.

[4]. Sathiamoorthy Manoharan, an empirical analysis of rs steganalysis, proceedings of the third international conference on internet monitoring and protection, ieee computer society washington, 2008.

[5]. Jithesh K , Dr. A V Senthil Kumar , Multi Layer Information Hiding - A Blend Of Steganography And Visual Cryptography, Journal of Theoritical and Applied Information Technology, 2010.

[6]. R. Chandramouli, Nasir Menon, Analysis of LSB Based Image Steganography techniques, IEEE-2001.

[7]. Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, " An Encrypto-Stego Technique Based secure data Transmission System", PEC, Chandigarh.

[8]. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems". Communication of the ACM, pp. 120-126, 1978.

[9]. Fridrich, J., Goljan, M. and Du,R, Reliable Detection of LSB Steganography in Color and Grayscale Images, Proceedings of ACM Workshop on Multimedia and Security, Ottawa, October 5, 2001, pp. 27-30.

[10]. Hardik Patel, Preeti Dave / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717.

[11]. T. Morkel, J. Eloff, and M. Olivier, "An overview of image steganography", In Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005).

[12]. J. Fridrich, M. Goljan, " Steganalysis of JPEG Images: Breaking the F5 Algorithm", Publisher: Springer Berlin, Heidelberg, Lecture Notes.

[13]. M. A. Bani Younes, A. Jantan, "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS, International Journal of Computer Science and Network Security, vol. 8 No. 6, June 2008.

[14]. J. Rodrigues, J. Rios, and W. Puech "SSB-4 System of Steganography using bit 4", In International Workshop on Image Analysis for Multimedia WIAMIS, May, 2005.

[15]. Takayuki Ishida, Kazumi Yamawaki, Hideki Noda, Michiharu Niimi, "Performance Improvement of JPEG2000 Steganography Using QIM", Department of System Design and Informatics, Journal of Communication and Computer, ISSN1548-7709, USA, Volume 6, No. 1(Serial No. 50), January 2009.