A Survey on Novel Visual Cryptographic Steganography Techniques

Shailendra M. Pardeshi
Assistance Professor
Department of IT,
RCPIT, Shirpur

ABSTRACT
The steganography and cryptography are the secret writing techniques. 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
Cipher Text, Cryptography, Novel, RSA algorithm, Steganography.

1. INTRODUCTION
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 [1]. 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 process of RS steganalysis uses the regular and singular groups as the considerations in order to estimate the correlation of pixels [2]. The presence of robust correlation has been witness in the adjacent pixels. But unfortunately using traditional LSB replacing steganography [3], 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 [4] [5], 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 [6]. 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. Such types of algorithms cannot persist without possessing appropriate characteristics in the visual cryptography procedure. The ground for this is that if the rebuilding method or even the encoding method changes the data exists in the image, then the system would accordingly change the encrypted information which makes the system feasible for extracting the encrypted data from the exposed image.

2. ENCRYPTION PROCESS
The encryption process takes the login data as input and also takes the key for encryption and performs the encryption using RSA algorithm and produces the output as encrypted text. The RSA algorithm uses binary key that are several hundred bits long, typically 512 bits. RSA takes a binary block of plain text of length smaller than the key length and produces a cipher text that is the same length of the key. Suppose P is an integer that corresponds to a block of plain text.RSA encrypts P as follows C=Pe (mod n) this process takes the encrypted text as input. The RGB components of the image are extracted which is fed to the fitness function stage [6]. Random selection function selects the pixels from the population randomly and provides the selected pixels as the input to the next stage. The pixels are selected by the genetic algorithm based on the threshold value determined by average value of pixels In the next stage the message data bits are hidden in the selected pixels.

Steps to encrypt embedded text into image

Input: Appended Encrypted text to insert.

Step 1: Get the char from the text convert it to its binary form

ch <- geth(text)

bit[ ]<-dectobin(ch)

Step 2: Get the pixel value and first bit of the bit variable

cbit[ ]<-bit[i]

Step 3: Check the value of the pixel value

Step 4: If LSB==1 && cbit ==1 Goto next step

Step 5: Else If LSB==1 && cbit==0

Step 6: Flip the pixel bit al LSB

Step 7: Else If LSB==0 && cbit==1

Step 8: Flip the pixel bit al LSB

Step 9: If LSB==0 && cbit ==0 Goto next step

Step 10: While there are still input goto step1

End

Output: Inserted image or watermarked image

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols [7]. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems.

3. 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.

The following formula provides a very generic description of the pieces of the steganographic process:

Cover Medium + Hidden Data + Stego_key = Stego_medium

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 [8].

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 [8] [9]. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed):

10010101	00001100	11001001
10010111	00001110	11001011
10011111	00010000	11001011

Note that it can hide 9 bits but at a cost of only changing 4 of the LSBs [9].

4. 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.

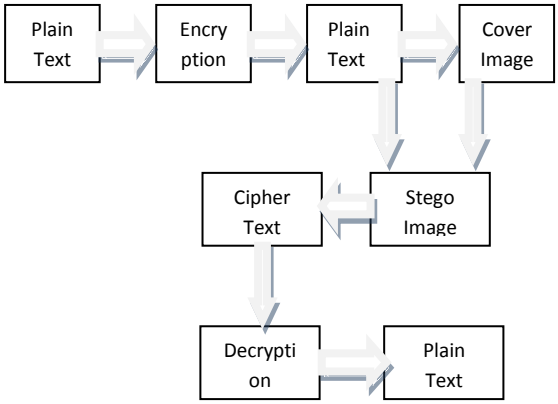

Figure 2: Combined concept of cryptography and steganography

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. A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2.In that both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. 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.

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].

5. RSA ALGORITHM FOR ENCRYPTION

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 [11]. 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.

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)

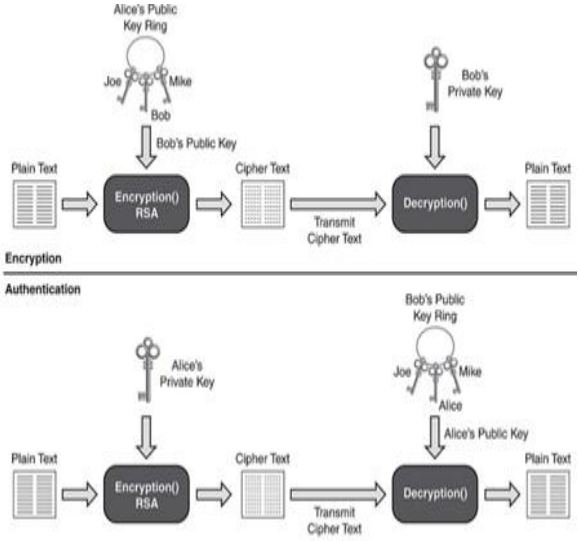

Figure 3: Example of RSA algorithm

6. OPERATION ON STEGO IMAGE USING DCT

In DCT based techniques, DCT coefficients are obtained for the given carrier image. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value [12] [13]. To avoid visual distortion, embedding of secret information that is avoided for the DCT coefficient value 0 [14].

Algorithm to embed text message:-

Step 1: Read cover image.

Step 2: Read secret message and convert it in binary.

Step 3: The cover image is broken into 8×8 block of pixels.

Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 5: DCT is applied to each block.

Step 6: Each block is compressed through quantization table.

Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.

Step 8: Write stego image.

Algorithm to retrieve text message:-

Step 1: Read stego image.

Step 2: Stego image is broken into 8×8 block of pixels.

Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 4: DCT is applied to each block.

Step 5: Each block is compressed through quantization table.

Step 6: Calculate LSB of each DC coefficient.

Step 7: Retrieve the data and convert each 8 bit into character [15].

7. 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.

8. REFERENCES

[1] 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.

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

[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] 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, 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] 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.

[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.