ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

A SECURE MAIL APPLICATION USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Vidhya Lakshmi R [*1] Selin M[2]
[*1]Computer Science and Engineering Department, KMEA College of Engineering, Edathala, India

KEYWORDS: Pretty Good Privacy, symmetric key cryptography, AES algorithm, Visual Cryptography, Shares, CFB mode of encryption, Adaptive Chosen cipher text attacks, Block ciphers

ABSTRACT

Although there are recent advancements in the development of messengers, Emails are the most widely used and popular messaging system used by the Internet users, which helps them to communicate in a short span of time. Security to the Email messages is an important issue as no Internet Standards provides security to the message content. The existing system, PGP (Pretty Good Privacy) used to encrypt and decrypt email messages, has a drawback of adaptive chosen cipher text attack as it works in CFB encryption mode as used by OpenPGP. To improve the security of email messages, a new model is proposed called as "A Secure Mail Application using Steganography and Visual Cryptography". The email message to be transmitted is converted to an image and shares are generated using (2, 2) Visual Cryptographic Technique. One of the shares is kept with the server and other is sent to the receiver's mail box. Man in the middle attack is not possible as these shares are transmitted through different medium. At the receiver side, two shares are fetched and decrypted to get the image. From this image, the original message is reconstructed. One added advantage of the system is that it ensures security of the shares by using AES algorithm, a symmetric key encryption method. The use of Image Steganography to construct an image from the message and use of Visual Cryptography provides secure email messaging.

INTRODUCTION

PGP (Pretty Good Privacy) [4] is a program for encryption and decryption of email messages. It ensures the message is not changed en route by providing a encrypted digital signature to identify the sender's identity. It uses the concept of hashing, data compression, symmetric key cryptography and public key cryptography. PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the session key that was used to encrypt the entire message. Both the encrypted message and the session key are sent to the receiver who first uses the receiver's private key to decrypt the session key and then uses that key to decrypt the message. Symmetric encryption in OpenPGP is performed using a variant of the standard Cipher Feedback (CFB) Mode for block ciphers. Adaptive chosen-cipher text attacks [7] on cryptographic protocols allow an attacker to decrypt a ciphertext C, getting the plaintext M, by submitting a series of chosen-ciphertexts $C\_\ \_= C$ to an oracle which returns information on the decryption. The ciphertexts can be adaptively chosen so that information on previous decryptions is available before the next chosen ciphertext is submitted. The attack on the OpenPGP CFB mode was able to obtain the entire plaintext using one oracle query which returned to the attacker the entire decryption of C'[1].

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

A new model is proposed namely "A Secure Mail Application using Steganography and Visual Cryptography". In this system, the message to be transmitted is converted into a gray scale image using steganography and shares are created using (2,2) VCS scheme from the image. The shares are encrypted using AES algorithm to ensure more security to shares. Both the shares are transmitted via different medium where one is sent to server and other to the receiver mail box. The cipher text is decrypted using the key to get the shares. The server and user shares are overlaid to get the gray scale image from which the original message is reconstructed.

The rest of the paper is organised as follows. Section II contains the brief description of Image Steganography and Visual Cryptography. Section III presents the proposed system. Section IV concludes the paper with the future works.

MATERIALS AND METHODS

The exiting email encryption system, PGP has many short comings. It is not secure and safe for email messages. Encryption is time consuming with public key cryptography. Man in the middle attack is possible when the data is transmitted; the information is fetched from within the network. As the PGP works in special CFB mode of Encryption, there is chance of adaptive chosen cipher text attacks where cipher texts are chosen adaptively and interactively before and after a challenge. Attacker sends a number of cipher texts to be decrypted, and then uses these results of decryption to select subsequent cipher texts. Large size message is the result of using this scheme.

In order to overcome these shortcomings, an e-mail application is proposed based on two security concepts – Image Steganography and Visual Cryptography. A Symmetric key cryptography algorithm, AES is used to enhance the security of the shares. The proposed system consists of three elements:

1. Steganography image for hiding the email message into the cover image.
2. Visual Cryptography shares created from the steganography image to ensure security.
3. Cipher text created as results of implementation of AES algorithm on the shares to enhance share security.

In the proposed system, when the user wants to send an email message, the system creates a gray scale image from the email message. Image steganography method is used to embed the email message contents and all the necessary details to be sent so that it reaches the intended person. The size of the message can be reduced to 1/5 of the original message using this method. The image is converted to shares using (2, 2) VCS scheme. User share is encrypted using AES algorithm for the share's security. Man in the middle attack is not possible as the shares are encrypted and they are sent using different transmission medium. One of the shares is sent to server and the other is sent to recipient mailbox.

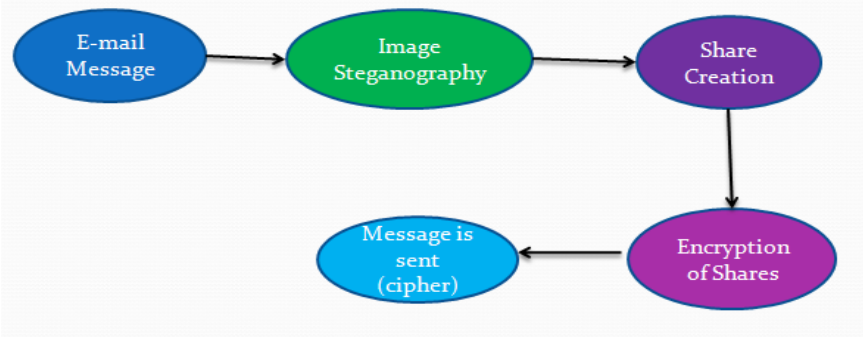
At the receiver side, the cipher texts are decrypted using the key to get the shares. Then shares are decrypted by overlaying the server shares with user share to obtain the gray scale image. The original message is reconstructed from this image. The proposed workflow of the system is given in Figure 1 as follows.

The different modules of the proposed system are as follows:

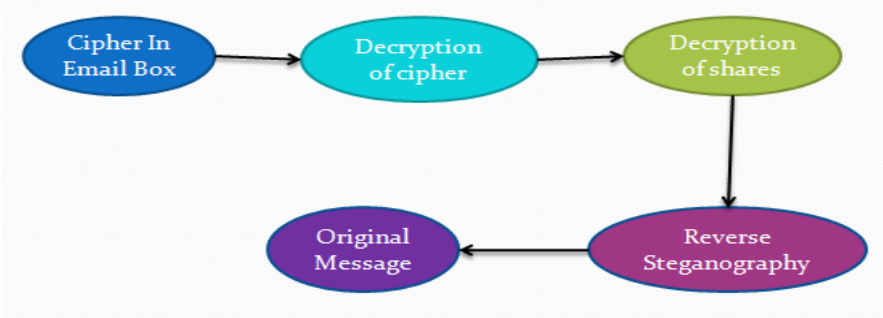
ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

A. Registration
B. Login
C. Image Steganography Modules
    a. Data embedding
    b. Date extraction
D. Visual Cryptography Modules
    a. Share Creation
    b. Share decryption
E. Share Security Modules
    a. Share encryption
    b. Share decryption



a. Sender side process



a. ***Receiver side process***

Fig 1. Proposed Design Flow(a) at the sender side (b) at receiver side

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

Registration
User signs up with the application by providing his details like userid, name, password, contact details etc. Validated information is stored in the database. If all data is valid, then registration is successful.

Login
When the user login to the system, user provides userid and password. Proper validation of data is performed. If authentication is valid, then login is successful.

Image Steganography Modules
The message composed will be converted to a stego image with all necessary information so that message reaches the right person. The message is embedded into an image that the user provides. Once it reaches the receiver, the image is regenerated from the shares and original message is reconstructed from the image. The most widely used LSB substitution method is used [10]. The algorithm to obtain the stego image is as follows.

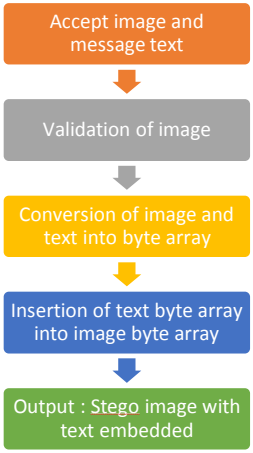


Fig 2. Image Steganograpghy Module

Visual Cryptography Modules
This module creates two shares using (2,2)VCS Thresholding scheme. One of the shares is kept with the server and other is sent to the mailbox of recipient. Only one with both the shares will be able to decrypt the shares making the system secure. Also shares are transmitted via different medium. Once the receiver needs to read the message, the shares are decrypted by stacking both the shares to obtain the stego image. The process is shown in the Figure 4 below. The image shares are created by taking the white and black pixels.

ISSN 2349-4506
Impact Factor: 2.265
Global Journal of Engineering Science and Research Management

The proposed system implements (2,2) Threshold VCS scheme to create shares. In this scheme, each pixel P in the original image is encrypted into two sub pixels called shares. Figure 3 shows the shares of a white pixel and a black pixel. The choice of shares for a white and black pixel is randomly determined. Single share doesn't provide any information about original message, since different pixels in the secret image will be encrypted using independent random choices. The value of the original pixel P can be determined when the shares are superimposed. If P is a black pixel, two black sub pixels are obtained. If it is a white pixel, one black sub pixel and one white sub pixel is obtained.

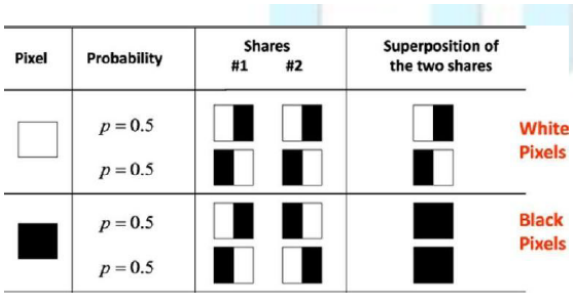


Fig 3. (2,2) VCS Thresholding scheme [2]

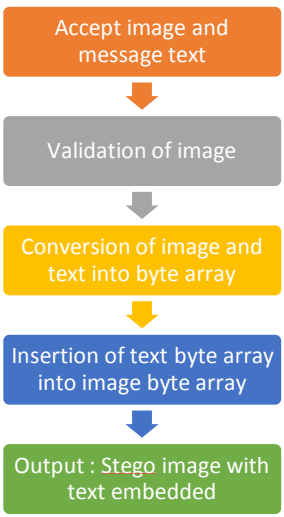


Fig 4. Share Creation Process

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

Share Security Modules

To increase the security of email messages, these modules are introduced. Using the AES algorithm on the shares, the system ensures more security of the data. A key is used to encrypt the shares and are also sent along with the mails. Keys ciphers used are block ciphers where 128 bit fixed block size is chosen. Key size of 128,192 or 256 bits specifies the number of repetitions of transformation rounds that converts the plain text to cipher text. The AES encryption process is shown in the Figure 5 below.

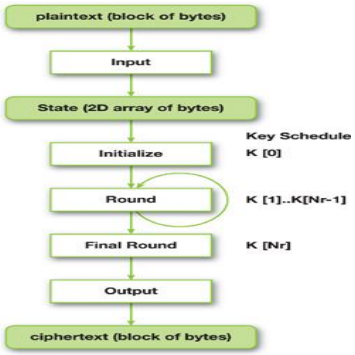


Fig 5. AES Encryption process

RESULTS AND DISCUSSION

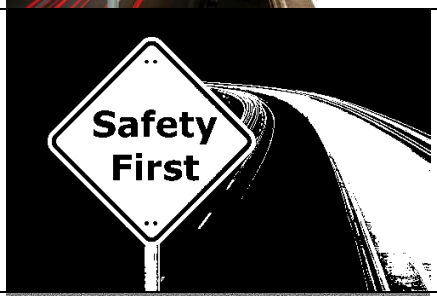
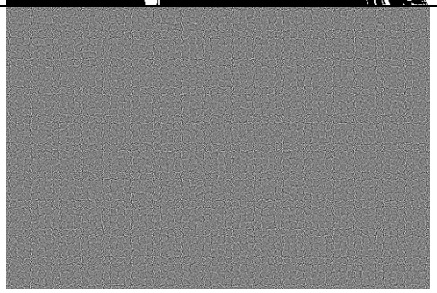
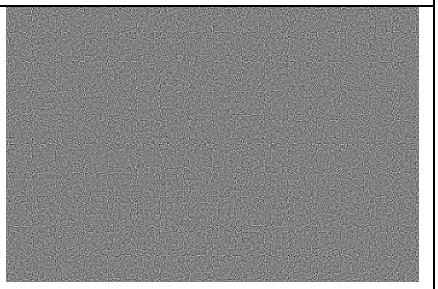
The email application is implemented as web server -client application. The emails are sent using standard internet protocols. The messages are saved in mail server from where user accesses his mails. Only send and receiving of mail texts are focussed. Additional functionalities need to be added to make it similar to existing real world email application. A database is used to store the personal details of the users using which validations of users are done during logging.

Tab 1. Results of the each Module

Message	Welcome to JAVA
Cover Image	

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

Output of Image Steganography Module	
Input to Visual Cryptography Module	
Output of Visual Cryptography Module	 User Share  Server Share
Output of Encryption of user share	Encrypted.png
Output at the receiver side after the reverse processes	Welcome to JAVA

CONCLUSION

PGP(Pretty Good Privacy) used for securing email messages are subjected to attacks as they work in CFB(cipher Feed Back) mode of encryption. A secure mail application is proposed based on three security concepts namely Image Steganography, Visual Cryptography and Symmetric Key Cryptography. The email message to be transmitted is

converted into a gray scale image using steganography and shares are created using (2,2) VCS scheme from the image. The shares are encrypted using AES algorithm to ensure more security to shares. Both the shares are transmitted via different medium where one is sent to server and other to the receiver mail box. The cipher text is decrypted using the key to get the shares. The server and user shares are overlaid to get the gray scale image from which the original message is reconstructed. So the proposed system ensures secure mailing.

Visual Cryptography can be extended to include more shares. Additional functionalities can be added to the system so that it will be similar to the existing Email Applications. System can be enhanced so that it is suitable to use in mobile environments. Cover images of different extensions can be used. The size of the image and shares can be reduced using compression mechanisms.

ACKNOWLEDGEMENTS

I am thankful to Mrs. Selin M, Associate Professor of Computer Science and Engineering Department, KMEA College of Engineering, Kerala for her keen interest and guidance in my paper.

REFERENCES

1. Ajish S, Rajasree R, "Secure Mail using Visual Cryptography", *IEEE* 33044,5Th *ICCCNT* 2014
2. M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
3. William Stallings, *Cryptography and Network Security, Pearson* Education Inc publishing as Prentice Hall.
4. P Zimmerman, *The Official PGP User's Guide, MIT Press, 1995*
5. Sandeep Katta, "*Visual Secret Sharing Scheme using Grayscale Images",* Department of Computer Science, Oklahoma State University Stillwater, OK 74078.
6. Seyed Hossein Kamali and Reza Shakerian," *A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", 2010 International Conference on Electronics and* Information Engineering (ICEIE 2010).
7. Serge Mister and Robert Zuccherato, "*An Attack on CFB Mode Encryption As Used By OpenPGP", Entrust, Inc., 1000 Innovation* Drive, Ottawa, Ontario, Canada K2K 3E7.
8. Souvik Roy1 and P. Venkateswaran2, "Online Payment System using Steganography and Visual Cryptography", ,2014 *IEEE* Students' Conference on Electrical, Electronics and Computer Science
9. Angel Freeda, "Image Captcha Authentication using Visual Cryptography" *IJREAT 2013*,Vol1
10. Nick Nabavian ,CPSC 350 Data Structures: Image Steganography , Nov. 28, 2007
11. Atul Sureshpant Akotkar, Chaitali Choudhary, "Secure of Face Authentication using Visual Cryptography", *International Journal of Innovative Science and Modern Engineering (IJISME)* ISSN: 2319-6386, Volume-2, Issue-5, April 2014
12. Avi Kak, Lecture 8: AES: The Advanced Encryption Standard, , February 18, 2015
13. Mrs. Rajashree M Byala, Mrs. Ramya Avinash,"Visual Secret Sharing For Hacking Prevention", *International Journal of Engineering Research & Technology (IJERT)* ,Vol. 2 Issue 5, May – 2013

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

14. *R Yadagiri Rao*, "Secure Visual Cryptography", *International Journal Of Engineering And Computer Science* ISSN:2319-7242 Volume 2 Issue 1 Jan 2013 Page No. 265-303
15. Nicholas G. McDonald, PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION: A Research Review
16. Adam Berent, Advanced Encryption Standard by Example
17. Shivani1, Mamta Sachdeva2, "A Study on Cryptography Aspects and Approaches", *IJCSMC*, Vol. 3, Issue. 9, September 2014, pg.482 – 488
18. http://en.wikipedia.org/wiki/Pretty_Good_Privacy
19. http://www.openpgp.org/about_openpgp/
20. http://www.pgpi.org/doc/pgpintro/
21. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack Ronald Cramer, May 1998
22. http://en.wikipedia.org/wiki/Adaptive_chosen_ciphertext_attack
23. Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Gangul1, Swarnendu Mukherjee and Poulami Das," A Tutorial Review on Steganography ", IC3–2008
24. Mehdi Hussain and Mureed Hussain ,"A Survey of Image Steganography Techniques ",*International Journal of Advanced Science and Technology*,Vol. 54, May, 2013
25. Parmar Ajit Kumar Maganbhai1, Prof. Krishna Chouhan, "A Study and literature Review on Image Steganography", *IJCSIT*, Vol. 6 (1) , 2015, 685-688
26. T. Morkel, J.H.P. Eloff, M.S. Olivier, "AN OVERVIEW OF IMAGE STEGANOGRAPHY"
27. Z. Zhou, G.R. Arce and G. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, No. 8, pp. 2441-2453, 2006.
28. Archana B. Dhole*, Prof. Nitin J. Janwe ,"An Implementation of Algorithms in Visual Cryptography in Images", *International Journal of Scientific and Research Publications*, Volume 3, Issue 3, March 2013
29. B.SaiChandana , S.Anuradha," A New Visual Cryptography Scheme for Color Images", *International Journal of Engineering Science and Technology*, Vol. 2(6), 2010, 1997-2000
30. Sozan Abdulla ,"New Visual Cryptography Algorithm For Colored Image" , Journal Of Computing, Volume 2, Issue 4, April 2010