INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ISSUES IN DATA HIDING AND IMAGE CRYPTOGRAPHY

MISS. PRUTHVIKA S. KADU[1], DR. H. R. DESHMUKH[2]

1. Master of Engineering, Computer science and Engineering Department, IBSS College of Engg., Amravati, India.
2. Prof. & Head Computer Science and Engg Department, IBSS College of Engineering, Amravati, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Maintaining the secrecy and confidentiality of pictures could be a spirited space of analysis, with two totally different approaches being followed, the primary being encrypting the pictures through encoding algorithms mistreatment keys, the opposite approach involves mistreatment data activity formula to keep up the pictures secrecy. A content owner encrypts the initial image mistreatment associate degree encoding key, and a information-hider will infix extra data into the encrypted image employing a data-hiding key thorough he doesn't recognize the initial content. With associate degree encrypted image containing extra information, a receiver could 1st decode it in step with the encoding key, so extract the embedded information and recover the initial image in step with the data-hiding key.

Keywords: Cover Image, Data Hiding, Data Extraction, Image Encryption, Image Decryption and Data Recovery.

Corresponding Author: MISS. PRUTHVIKA S. KADU

Access Online On:

www.ijpret.com

How to Cite This Article:

Pruthvika S. Kadu, IJPRET, 2015; Volume 3 (9): 431-435

PAPER-QR CODE

INTRODUCTION

The process of hiding information inside another media is called stegnography. The media with secret information is called stego media and without hidden information is called cover media[1]. Stegnography has a long history of been used as a way to protect security and privacy of valuable information. While cryptography focuses on protecting the secret message by jumbling its content, stegnography concerns on protecting the secret message by concealing its mere existence. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego signal. At the receiver's end, the secret data can be recovered from the stego signal using different algorithms[2].

Cryptography is a technique for securing the secret information. Sender encrypts the message using the secret key and then sends it to the receiver. The receiver decrypts the message to get the secret information. Cryptography focuses on keeping the content of the message secret where as data hiding concentrates on keeping the existence of the message secret [3]. Visual Cryptography using XOR operation provides more security than other approaches. Because XOR operation can be implemented by four NOTs and three ORs[11][12]. Data hiding is the other technique for secured communication. Data hiding involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information [4]. Data hiding is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly.

The strength of data hiding gets amplified if it combines with cryptography. The terminologies used in data hiding are cover-image, hidden image, secret message, secret key and embedding algorithm. Cover-image is the carrier of the message such as image, video or audio file. Cover-image carrying the embedded secret data is the hidden image. Secret message is the information that is to be hidden in a cover image. The secret key is used to embed the message depending on the hiding algorithm [4]. The embedding algorithm is the way, which is used to embed the secret information in the cover image.

The security of the transformation of hidden data can be obtained by two ways: encryption and data hiding. A combination of the two techniques can be used to increase the data security. In

encryption, the message is changed in such a way so that no data can be disclosed if it is received by an attacker. Whereas in Data hiding, the secret message is embedded into an image often called cover image, and then sent to the receiver who extracts the secret message from the cover message. When the secret message is embedded into cover image then it is called a hidden image. The visibility of this image should not be distinguishable from the cover image, so that it almost becomes impossible for the attacker to discover any embedded message.

LITERATURE SURVEY

Fridrich et al. (2001) [5], proposed the reversible data embedding method for the authentication purpose so the embedding capacity of this method is low. To separate the data extraction from image decryption, Zhang emptied out space for data embedding in the idea of compressing encrypted images [6], [7].

An encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes, a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in [7]. W. Liu, W. Zeng, the lossy compression method presented in [7], an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied X. Zhang[10].

W. Liu, W. Zeng proposed, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource, a lossless compression method for encrypted gray image using progressive decompose and rate compatible turbo codes is developed in [7].

The method in [8] compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is the spatial correlation of decrypted images.

A novel method for RDH in encrypted images, for which we do not “vacate room after encryption” as done in [9], but “reserve room before encryption”. In that, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to

embed data. In methods of [8]–[9], the encrypted 8-bit gray-scale images are generated by encrypting every bit-planes with a stream cipher.

CONCLUSION

The aim of the present work is therefore to propose and experimentally evaluate an combine approach of encryption and data hiding scheme to increase and improve hiding capacity of image carrier. The main aim of the proposed model is to improve security, reliability and efficiency of secret message. Comparative methods for encryption and data hiding are also provided. The methods were closely observed for their limitations and based on this a new method is proposed to achieve the goal which combines the two approaches of Image cryptography and data hiding. The proposed method is expected to offer better results over any of the available technique.

The advantage of both the techniques discussed can be concentrated and extended to improve upon the results depending on the end application requirements supporting security, authentication and authorization.

REFERENCES

1. V. Saravanan and A. Neeraja, “Security Issues in Computer Network and Steganaography”,2013 IEEE :978-1-4673-4603-0/12

2. Birgit P tzmann, Information hiding terminology-results of an informal plenary meeting and additional proposals, Proc. of the First International Workshop on Information Hiding, vol. 1174, pp. 347-350. Springer, 1996.

3. Cachin, C.: An information-theoretic model for steganography. In: Aucsmith, D. (ed.) IH 1998. LNCS, vol. 1525, pp. 306-318. Springer, Heidelberg, 1998.

4. Lini Abraham, Neenu Daniel ,” Secure Image Encryption Algorithms: A Review”, International Journal of Scientific & Technology Research volume 2, issue 4, April 2013, PP-186-189.

5. Mohanraj Arumugam and Rabindra Kumar Singh, “Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image” IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013, PP-1-5.

6. Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G., 2008. A novel difference expansion transform for reversible data embedding. IEEE Transaction Information Forensics and Security 3(3), 456–465.

7. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. SignalProcess.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

8. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

9. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1,pp. 53–58, Feb. 2011.

10. X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

11. X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

12. P. Tuyls, H. D. L. Hollmann, J. H. Van Lint, and L. Tolhuizen, "XORbased visual cryptography schemes," *Designs Codes Crypt.*, vol. 37, no. 1, pp. 169–186, 2005.

13. D. S. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognit.*, vol. 40, no. 10, pp. 2776–2785, 2007.