ABHIYANTRIKI
An International Journal of Engineering & Technology
(A Peer Reviewed & Indexed Journal)
Vol. 3, No. 2 (February, 2016) http://www.aijet.in/ eISSN: 2394-627X

Survey on Improving Security of Images with the Combination of Encryption and Steganography

Dhvani C. Panchal*
ME Scholar
KIRC, Kalol, India

Chaita Jani
Assistant Professor
KIRC, Kalol, India

Hemin Panchal
BE Scholar
GIT, Gandhinagar, Kalol, India

Abstract

Security is major concern for transmission of multimedia data in IT field. Some of the possible solutions for securing the multimedia data during the transmission are: encryption, steganography, watermarking, encoding, authentication etc. All these techniques provide security up to some satisfactory level for protecting multimedia data. Paper is focusing on different approaches with the combination of encryption and steganography for the purpose of improvement of security. Encryption and Steganography are used in such a way that security of the systems is improved at some level. Paper briefly describes some of the approaches already available with the combination of encryption and steganography techniques.

Keywords*: Image Encryption, Image Decryption, Steganography, Encryption Key, Stego Key.*

****Author for correspondence*** dhvanipanchal28@gmail.com

1. Introduction

In multimedia transmission, the sending and receiving of multimedia data is not so easy. As the data exchange in electronic way is rapidly increasing, it is also important to protect the confidentiality of data from unauthorized access. This exchange process has pass through some complexities like data integrity, non-repudiation, authentication, authorization, active/passive attacks, snooping from intruder etc. Many cryptographic techniques are available for providing the security of images. Encryption, authentication, key distribution, steganography, etc. are some of cryptographic techniques. One technique used here is encryption. Hence encryption of data is done to confirm security in open networks such as the Internet where the multimedia applications are ever growing day by day. Image encryption is a technique that provides security to images by converting the original image into an image which is difficult to understand. That is converting input image into cipher image which is un-recognizable form. Applications of image encryption can extended to military communication, multimedia systems, medical science, telemedicine, Internet communication etc. [1]. Image encryption techniques can be divided into two groups

based on the approach used to construct the encryption scheme: chaos based methods and non chaos based methods. Image encryption can also be classified according to the percentage of the data that is encrypted as full encryption and partial encryption. Another technique here used is steganography. Steganography is an art of hiding secret information inside a carrier like image, audio, video. Image steganography is technique of hiding data into image. Hidden data can be in the form of text, image, video, audio etc. The text data is used as hidden information here and image is used as a carrier. Image Steganography can be represented as 'Stego-image = Cover image + Secret message + Stego key'. Stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties who know it. With the help of Stego key the text data which we want to hide into cover medium is embedded without affecting the cover image. The aim of steganography is that the cover medium must not change. Digital images are one of the common and most popular ones due to their frequency on the Internet and high capacity of data transmission without degrading effect on images quality. It is a high security technique for long data transmission. The paper provides a brief introduction of some approaches which are developed with the goal keeping in mind to improve security of data with the combination of encryption and steganography. Different approaches used different input data for encryption and steganography.

2. Review of Literature

Pooja Rani and Apoorva Arora have been used hybrid image security approach. The techniques included in the combination are image compression, cryptography and steganography. DWT compression has been used, due to its strongest strength for compression algorithm. The steganographed image has been compressed for reducing its size. Blowfish encryption algorithm used for the encryption purposes. It also offers maximum throughput and energy efficiency. Compressed image has been encrypted to enhance the image security and original image has been hidden into another image. A cluster based steganographic technique was used. The original image and face image has been analyzed, and the original image was embedded in those areas of face image, where color schemes of the real image and face image was most similar. Hierarchical clustering is used for clustering technique [2]. Satwinder Singh and Varinder Kaur Attri presented the dual layer of security for data, in which first layer is to encode data using Least Significant Bit (LSB) image steganography technique and in the second layer encryption of the data using Advance Encryption Standard Algorithm (AES). Steganography does not replace the encryption of data, instead it provides extra security feature to it. In their work secret text message is hiding behind the digital image file and this image file is then encrypted using AES encryption algorithm [3]. Vinit Agham and Tareek Pattewar introduced a new way for originating the existing concept i.e. separable reversible data hiding. Mainly, the concept of separable reversible data hiding technique is based on steganography. The main objective of this literature is to work on the concept in which they used text as a hidden data, no plain spatial domain is used here, attempt to increase the amount of data which is to be hide, evaluating quality by different interpretations. The principal notion of separable reversible data hiding is consisting three key procedures. They do encryption of cover media then hide the data and finally get the data as well as cover media as per provisions [4]. Rupesh Gupta and Tanu Preet Singh proposed a new method by combining three security techniques i.e. steganography, cryptography, and watermarking, it will not only hide the information but produce better results for MSE. It is also shown that PSNR and Embedding capacity still after the noise attack. They

worked on various parameters like PSNR, MSE and Embedding capacity which proved better results than the traditional approach [5].

R. Nivedhitha & T. Meyyappan proposed the combination of encryption and steganography by using the DES algorithm and LSB technique. DES is basically used to encrypt secret image and LSB technique is used to hide encrypted secret image into cover image. To produce better imperceptibility this proposed method provides a higher similarity between cover and stego images as a result. It is hardly attracted from eavesdropper by naked eye when these two techniques are combined. Finally the proposed technique is effective for secret data communication [6]. Md. Rashedul Islam et al. developed a new technique to hide large data in Bitmap image using filtering based algorithm. This method uses the concept of status checking for the purpose of insertion and retrieval of message. It is being predicted that the proposed method will able to hide large data in a single image consisting advantages and avoiding disadvantages of traditional LSB method. Hence the proposed Steganography technique is very efficient to hide the secret information inside an image [7]. Gunda Sai Charanl et al. proposed a highly secured chaos based image steganography technique. Encryption has been added to steganography technique at two levels because of Ceaser cipher and Chaos encryption technique. The proposed algorithm uses cover in the spatial domain for hiding secret information. Proposed algorithm has added security and better performance when compared with base 3, 3, 2 LSB steganography technique [8]. Ashwini B. et al. provided DCT which is used for lossy compression and for encryption of secret data block ciphers are used. Although these approaches are relatively secure, but high processing is required, it involves computational overheads and processing speed is less. Here, a hybrid approach of Compression, Double-Encryption and Steganography is combined to increase encryption speed, reduce processing time and also provides more security, authentication, authorization, integration of data and also maintains confidentiality [9]. Priya Bharti and Roopali Soni proposed a novel scheme for the embedding data in images they first encrypt data and then embed it with image with the help of Steganography algorithm. The method is much efficient when applied to those images whose pixels are scattered homogeneously. Here, the given image is partitioned into four block levels, and then the data will be embedded into selected the four diagonal sub-blocks values depending upon key. This algorithm only requires minor steps and it can embed data more efficiently. The quality of stego-image is greatly improved when this algorithm is used [10].

3. Conclusion

In today's world where nothing is secure, the security of multimedia data is very important. We have surveyed different latest image encryption & steganography approaches which are implemented on the basis of combination of traditional techniques. We can conclude that all these approaches and their used techniques are good for encryption and steganography regarding their functionality. They all have their own advantages and disadvantages. The common goal of improving security behind all these approaches is satisfied up to some satisfactory level with the combination of encryption and steganography.

References

[1] Minal Govind Avasare, Vishakha Vivek Kelkar," Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, 2015.

[2] Pooja Rani and Apoorva Arora, "Image Security System using Encryption and Steganography", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June 2015.
[3] Satwinder Singh and Varinder Kaur Attri, "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 5, 2015, pp. 259-266.
[4] Vinit Agham and Tareek Pattewar, "A Novel Approach towards Separable Reversible Data Hiding Technique", International Conference on Issues and Challenges in Intelligent Computing Techniques, 2014.
[5] Rupesh Gupta and Tanu Preet Singh, "New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters", International Conference on Contemporary Computing and Informatics (IC3I), 2014.
[6] R. Nivedhitha, T. Meyyappan, "Image Security Using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, Vol. 3, Issue 3, 2012.
[7] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", 3rd International Conference on Informatics, Electronics & Vision, 2014.
[8] Gunda Sai Charanl, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V, Divya Lakshmi K, "A Novel LSB Based Image Steganography With Multi-Level Encryption ", 2nd International Conference on Innovations in Information Embedded and Communication Systems, 2015.
[9] Ashwini B, Pushpalatha S, R H Goudar, "A Hybrid Approach for Enhancing Data Security by Combining Encryption and Steganography", Proc. of the Intl. Conf. on Advances In Engineering and Technology, 2014. doi: 10.15224/ 978-1-63248-028-6-01-19
[10] Priya Bharti and Roopali Soni, "A New Approach of Data Hiding in Images using Cryptography and Steganography", International Journal of Computer Applications, Vol. 58, No. 18, 2012.
[11] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, (1999). "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078.
[12] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen," A chaos-based digital image encryption scheme with an improved diffusion strategy", Optical Society of America, Vol. 20, No. 3, pp 2363 – 2378, 2012.
[13] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal, "A Review on Different Image Steganography Techniques", International Journal of Engineering and Innovative Technology, Vol. 3, Issue 7, January 2014.
[14] Abhinav Srivastava, "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 6, June 2012.