
ABSTRACT

Internet is the popular communication media now a days but message transfer over the internet is facing some problem such as data security, copyright control, data size capacity, authentication etc. Data hiding plays an important role in data security. It is a process in which secret data or information is stored or hidden into cover media. And so many researches are progressing on the field like internet security, steganography, and cryptography. When transfer the secure data over an insecure channel it is needed to encrypt cover or original data and then embed the secure data into that original or cover image. This project introduces the new way of originating the previous concept i.e. separable reversible scheme for data hiding.

Actually, the separable reversible data hiding technique is based on steganography and related with internet security. Data hiding process is a combination of set of the embedded secret data and a set of the cover media or original image. The main objectives of this literature is to work on the concept in which we used text as a hidden data, attempt to increase the amount of data which is to be hide in the cover image, evaluating quality of image by different interpretations. The principle of separable reversible data hiding is consisting of three key procedures. First is encrypt the cover image second hide the data in encrypted image and last extract the secret data from the cover image.

KEYWORDS: Image encryption, image recovery, reversible data hiding, separable reversible data hiding, PSNR.

INTRODUCTION

Now days the data security and data integrity are the two challenging areas for research. There are so many research is progressing on the field like internet security, steganography. Sometimes we found certain distortion in images used in military, medical science which is un-acceptable. Hence for data hiding there are different techniques using which we can extract secret data or information correctly and after that original cover image content can be correctly recovered. Is called as reversible data hiding technique and is also called as lossless, distortion free and reversible data hiding technique which enables the exact recovery of the original signal with the extraction of the secret information. And this type of exact recovery without any loss of data is nothing but the reversible data hiding. Usually, the well-known LSB (least significant bits) method is used as the data embedding method. Many times reversible data hiding is mainly used for the authentication purpose.

SEPARABLE REVERSIBLE DATA HIDING TECHNIQUE

The term "reversible data hiding" means getting the exact recovery of the data after performing the operation like encryption-decryption and data hiding in cover image. Now the most important question is; what is mean by "separable reversible data hiding technique"? The word separable means it separates or divides two major activities in the scheme. These two activities like separating data and cover image are getting the exact recovery of the secure hidden data and exact recovery of cover data or original image which is used to hide as shown in Fig. 1.

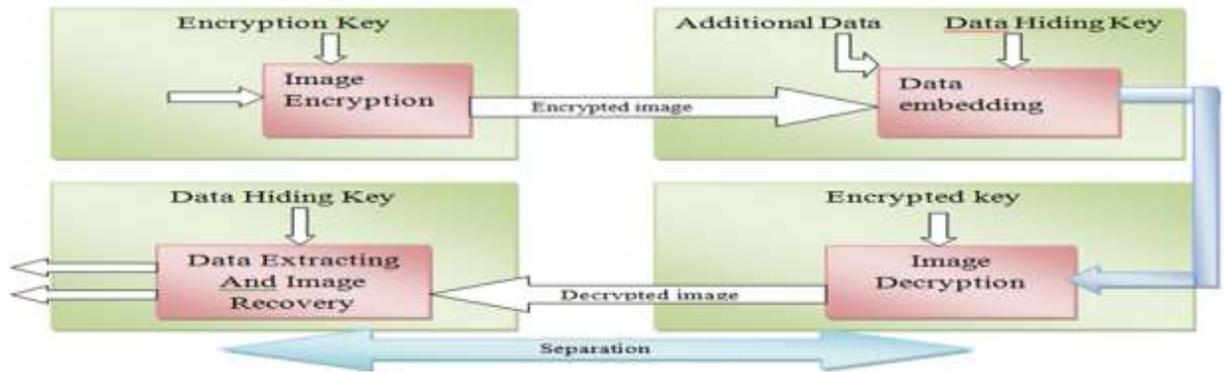


Fig1. Separable reversible data hiding

By using separable reversible scheme secret data is hidden into a cover media. The data may be any text related to the image such as authentication data or information. At the receiver side it must be able to extract the hidden or secret data from the cover image. In some different applications such as medical, military, it is highly desired that the original image should be perfectly recovered after data extraction. The separation of extracting the data and getting the cover image or media come to be exists. Hence this is known as Separable Reversible Data hiding technique.

LITERATURE SURVEY

Previously, data to be transmitted were encrypted using the algorithms like DES, Triple DES. They provided the data protection but up to certain extent. DES algorithm consumes least decryption time. It is a secret key like private key based algorithm which experiences problems like key distribution and key agreement but provide throughput in less power intake [8]. The Protective measure of highly secret data is on demand in the market. On the other hand data can be secret by using data hiding techniques. Data hiding techniques embeds the data into cover objects or original image like texts, images, audios, videos. For more protection, cryptographic techniques can be applied to an information hiding scheme to encrypt the secrete information. Stereography can be used to increase the chances to hide the data so that the hackers are not able to get the secret information which is hidden behind the image [9].

The data hiding process is made of image encryption, data embedding and data extraction/image recovery like cover object. The sender encrypts the original image or cover object using an encryption key to produce an encrypted image or in unreadable format. After that, the data hider compresses the (LSB) least significant bits of the encrypted images using a data hiding key to create a more space to adjust the extra data.

At the receiver side, the embedded data in the created space can be easily extracted from the encrypted image containing additional data with the help of data hiding key. By using both of the encryption process and data-hiding keys, the embedded additional data can be recovered and the cover image can be perfectly restored [4]. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be extracted and the original content of the encrypted image that contains secret data.

In reversible data hiding using optimal value transfer techniques, the values of sender image are changed and original content of the image can be correctly restored after extracting the data on the receiver side [8]. According to this technique, the optimal constraint of value alteration using a payload-distortion criterion is founded by using the iterative procedure, and a reversible practical data hiding scheme was proposed [7]. The secret data, and the auxiliary information used for recovering the secret data, were carried out by the differences between the original pixel-values and the corresponding values [8]. By using this technique, a good performance is obtained for the reversible data hiding. In this scheme, the secret information and the auxiliary data used for data recovery [8].

The optimal value transfer matrix is generated for increasing the amount of secret data or information, i.e. payload. It also stated that the size of auxiliary data can not affect the optimality of the sending matrix. By pixel division in the original image or cover image is divide into two different sets and a number of different subsets, the hiding the secret

data is performed in the subsets generated from cover image, and then the auxiliary data or information of a subset is always produced [7]. Similarly, the receiver could successfully extract the embedded secret information and could extract the original content or data in the subsets with an inverse order.

According to the novel scheme of separable reversible data hiding, at sender side encrypts the original image or cover image using an encryption key. Then, secret data is hidden behind the image. Now, the encrypted image consist of the additional information or data, if the receiver has a data-hiding key, then he can recover the additional data or information though he does not have an any idea related to the cover image content [6]. At the destination, if the receiver has an encryption key, then the receiver can easily decrypt the received data or information so that obtain the image similar to the original image or cover image.

The sender also called as the content owner encrypts the original or cover uncompressed image by using the image encryption algorithms and by using a key called as the encryption key to generate an encrypted image means unreadable format. At the other side, the hidden data in the image can be extracted easily from the encrypted image containing additional data or information according to the data-hiding key [10]. When encryption and data-hiding keys are used by receiver, the confidential data embedded can be extracted successfully and the cover image can be recovered correctly [8].

REFERENCES

- [1] Sumedha Sirsikar, " Analysis of data hiding using Digital Image Signal Processing" , IEEE, 2015.
- [2] Rintu Jose, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance", IEEE, 2015.
- [3] Prof. Dan Meng High, "Capacity Reversible Data Hiding in Encrypted Images", IEEE, 2015.
- [4] Priyadarshni, "A hybrid data hiding scheme to enhance the capacity of one-third probability embedding method", IEEE, 2015.
- [5] Miss. Priyanka V Deshmukh, "Higher LSB Optimize Data Hiding Mechanism on Encrypted Image", IEEE, 2015.
- [6] Shri Lakshmi Pravalik, "LSB Based Reversible Data Hiding Technique", IEEE ,2014.
- [7] Vinit Agham, "Data Hiding Technique By Using RGB LSB Mechanism", IEEE ,2014.
- [8] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2013.
- [9] Dipesh Agrawal and Samidha Diwedi Sharma "Analysis of Random Bit Image Steganography Techniques "International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology – 2013.
- [10] 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.
- [11] X Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 826-832, Apr. 2012.
- [12] Beenish Mehboob and Rashid Aziz Faruqi, " A Steganography Implementation", IEEE 2008 M.B. Ould MEDENI, El Mamoun SOUIDI, " A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution "IEEE 2010.
- [13] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2706–2722, Jun. 2008.
- [14] S. K. Moon and R.S. Kawitkar, "Data Security using Data Hiding", IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.
- [15] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, Mar. 2006.
- [16] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2706–2722, Jun. 2008.
- [17] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.

- [18] J. Tian, "Reversible data embedding using a difference expansion, "IEEE Trans. Circuits Syst. Video Technol." 13, no. 8, pp. 890-896, Aug. 2003.
- [19] Mohammad Awrangjeb, "An Overview of Reversible Data hiding", ICCIT, Jahangirnagar University, Bangladesh, pp. 75-79, Dec. 2003
- [20] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," IEEE Trans. Multimedia, vol. 3, no. 3, pp. 273-284, Sep. 2001.
- [21] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum Detection structure," IEEE Trans. Multimedia, vol. 3, no. 3, pp. 273-284, Sep. 2001.
- [22] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images Detector performance analysis and a new structure," IEEE Trans. Image Process., vol. 9, no. 1, pp. 55-68, Jan. 2000.
- [23] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1062-1078, Jul. 1999.