Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.164 – 169

SEPARABLE REVERSIBLE SCHEME FOR DATA HIDING IN IMAGE

Pratiksha S. Kale[1], Prof. Mahip M. Bartere[2]

[1]Master of Engineering Scholar, Computer Science & Engg, Department

G. H. Raisoni College of Engg and Management, Amravati, India

[2]Guide, Computer Science & Engg., Department

G. H. Raisoni College of Engg and Management, Amravati, India

[1] pratikshakale48@gmail.com; [2] Mahip.bartere@raisoni.net

Abstract— Internet is the popular communication media now a days but message transfer over the internet is facing some problem such as copyright control, data security, data, 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 or confidential 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.

Keywords— Image encryption, image recovery, reversible data hiding, separable reversible data hiding, embedded data.

I. 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.

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.

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.

Steganography is the process of hiding a secret data in such a way that someone cannot know the presence or contents of the hidden data or message. Technically in simple word "steganography means hiding data within another".

In some cases, administrator needs to add some additional message or secret data, such as the original information, authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side [11].

II. 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. The Protective measure of highly secret data is on demand in the market. On the other hand, in AES algorithm uses least memory usage. On the other hand data can be confidential 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 [10].

The data hiding process is made of image encryption, data embedding and data extraction/image recovery like original image or cover object. The sender encrypts the original or cover image 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 secretor confidential 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 [8]. The secret data or confidential image, 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 [7].

By using this technique, a good performance is obtained for the reversible data hiding. In this scheme, the secret or confidential 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. Many techniques are used to hide data in various formats in steganography. The many times used mechanism on account of its simplicity is the use of the Least Significant Bit. This method is for normally used to hide data in a digital image.

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].

According to the novel steganographic method for hiding data within the spatial domain of the grayscale image the proposed approach works by dividing the cover image or original image into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four

bits of the pixel. The results have shown that the proposed method not only has an acceptable image quality but also provides a large embedding capacity hence data hiding capacity is improved.

III. PROPOSED METHODOLOGY

A. Data Hiding:

- Data hiding is the process of hiding secret data in cover image so that we get the stego image.
- Stego image is a combination of secret image and carrier image.

Step1: Take image as a cover image for hiding secret image.

Step2: Input secret image

Step3: Encrypt secret image by applying encryption algorithm

Step3: Convert secret data in binary format.

Step3: Hiding secret data in cover image using data hiding algorithm.

Step4: We will get the stego image.

Step5: Encrypt stego image by applying encryption algorithm.

Step5: Finally, we will get the stego encrypted image.

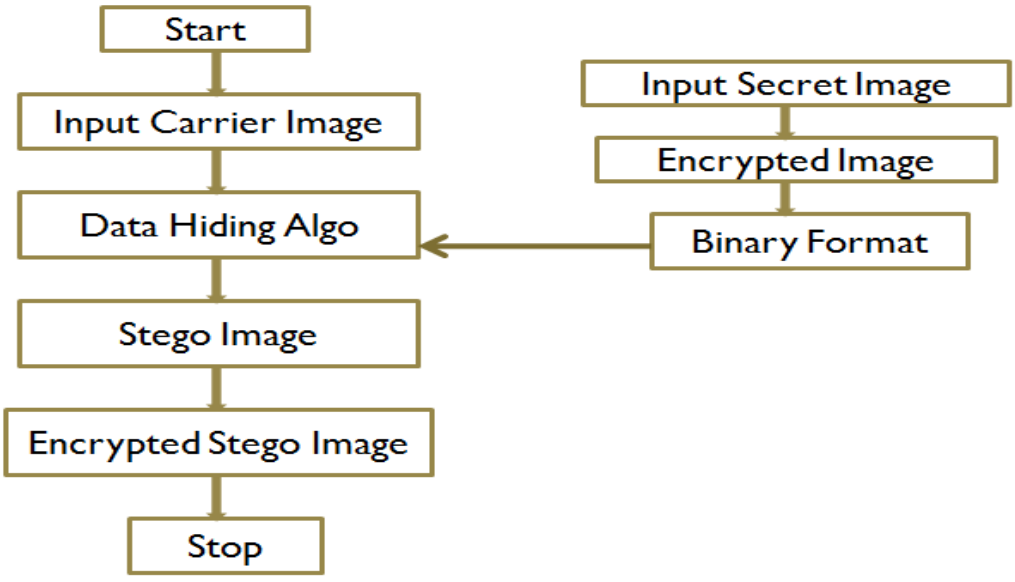

Fig 1: Data Hiding Process

B. Data Extraction:

Data Extraction is the process of extracting secret image from encrypted stego image for this purpose there is need to decrypt it first.

Step1: At the receiver side we will get the encrypted stego image.

Step2: Decrypt encrypted stego image.

Step3: At this stage, extract data.

Step4: Now, convert extracted data in ASCII format.

Step5: Finally, we will get the original secret image which hidden under the carrier image.

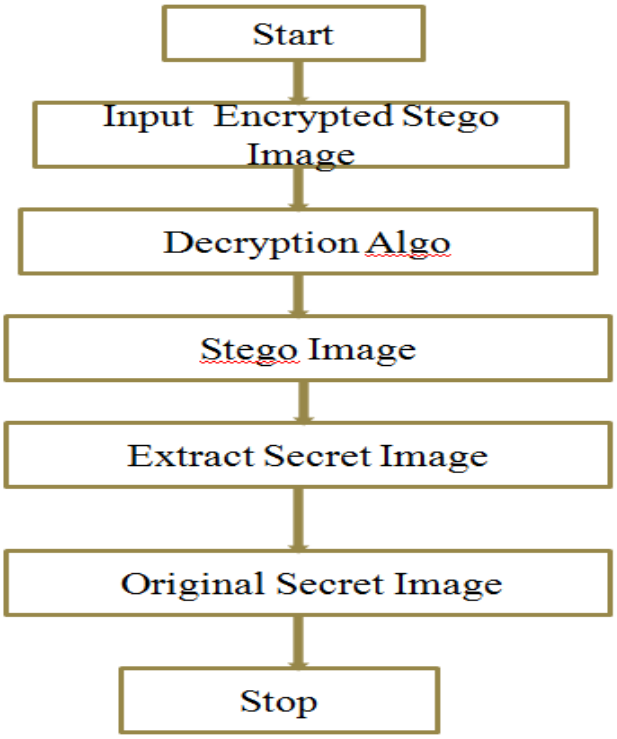

Fig 1: Data Extraction Process

References

[1] J. Tian, "Reversible data embedding using a difference expansion, "IEEE Trans. Circuits Syst. Video Techno! VO!' 13, no. 8, pp. 890-896, Aug. 2003.

[2] Mohammad Awrangjeb, "An Overview of Reversible Data hiding", ICCIT, Jahangirnagar University, Bangladesh, pp. 75–79, Dec. 2003.

[3] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vo!. 52, no. 10, pp. 2992-3006, Oct. 2004.

[4] H.-C. Wu, N.-I.Wu, C.-S.Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Techno!., vo!' 16, no. 3, pp. 354-362, Mar.2006.

[6] 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.

[7] BeenishMehboob and Rashid Aziz Faruqui," A Stegnography Implementation", IEEE 2008.

[8] W. Liu, W. Zings, L. Dong, and Q. Yao, " Efficient compression of encrypted grayscale images" , IEEE 2010.

[9] M.B. Ould MEDENI, "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution "IEEE2010.

[10] Smitha, M., Jayanthi, V.E., Merlin A, "Image encryption using separable reversible data hiding scheme," Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), vol., no., pp.1, 6, 4-6 July 2013 .

[11] M,Dr. V.E. Jayanthi, "encryption using separable reversible data hiding scheme", IEEE 2013.

[12] 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.

[13] 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.

[14] Shri Lakshmi Pravalik, "LSB Based Reversible Data Hiding Technique", IEEE ,2014.

[15] Vinit Agham, "Data Hiding Technique By Using RGB LSB Mechanism", IEEE ,2014

[16]Vinit Agham, "DATA HIDING TECHNIQUE BY USING RGB LSB MECHANISM", ICICES2015.

[17] Sneha A. Deshmukh, "An Authentication of Secretely Encrypted Message Using Half-Tone Pixel Swapping From Carrier Stego Image", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2409-2015.

[18] Sumedha Sirsikar, " Analysis of data hiding using Digital Image Signal Processing" , IEEE, 2015.

[19] Prof. Dan Meng High, " Capacity Reversible Data Hiding in Encrypted Images", IEEE, 2015.

