A Review on Separable Reversible Data Hiding in Encrypted Image

Swapnil W. Daware
Department of Computer Science
Lumbini group of institutions
Anatharam, Bhongir, Nalgonda, Telangana, India
E-mail: swapnildaware009@gmail.com

Prof. Ajay Kumar Kurra
Head of Department of Computer Engineering
Lumbini group of institutions
Anatharam, Bhongir, Nalgonda, Telangana, India
E-mail: ajaykumarkurra@gmail.com

***Abstract*—**This work proposes a new system for separable reversible data hiding in color images encrypted with the approach of adding the matrix. In the proposed scheme, Take color image input and provide the encryption key to encrypt the picture image and then compressed encrypted with various algorithms. Due to the compression of the image to create a sparse space to accommodate the additional data, integrated data using the key data hiding. If the receiver has the encryption key, you can decrypt the received data to obtain the image only. If the receiver has the data hiding key, it can extract data only. If the receiver is both the key to hidden data and the encryption key, it can extract the additional data and recover the original content without any errors using the spatial correlation in the natural image if the amount of data extra is great.

Keywords-*Encryption, decryption, compression, reversible-data hiding.*

*****

1. INTRODUCTION

The usage of internet is increasing day by day as peoples understand the importance of internet. Number of users also increasing though internet is very useful in business activity, communication over the internet is facing some problem such as data security, copyright control, data size capacity, authentication etc.[7]. Here we are investigating separable reversible data hiding in encrypted domain in which we use image as a cover medium. Xinpeng Zhang presented a unique reversible (lossless) data hiding (embedding) technique, which enables the exact recovery of the original host signal with the extraction of the embedded information. And this exact recovery with lossless data is nothing but the reversible data hiding. The LSB method is used as the data embedding method. Reversible data hiding is a technique that is mainly used for the authentication of data like images, videos, electronic documents etc. The application of reversible data hiding technique is in IPR protection, authentication, military, medical and law enforcement.

A. Data Hiding: Data hiding means to hide data sometimes also referred as Steganography. Two types of data is being hided, one is an embedded data and another is cover media data. Sometimes, the cover media becomes distorted due to data hiding andcannot be inverted back to the original media. That is, cover media has permanent distortion even after the hidden data have been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques [9].

B. Reversible Data hiding: Reversible data hiding is a technique in which data is embedded into image in reversible way. Normally if the data is huge and we have to transfer it on the internet then conventional way of data hiding is at first we must compress the that data and then encrypt it but in reversible data hiding method we have to encrypt the image and then compress it that's why named reversible data hiding.

C. Separable Reversible data hiding: In the separable reversible data hiding technique, first of all sender sends encrypted image and at the receiver side there are three choices for receiver. If the receiver wants only image then receiver can use encryption key also if he or she want only data which is embedded into image then he or she can use data hiding key or if he or she want both encrypted image and data hidden behind that image then he or she can use both keys. That's why it is named as separable reversible data hidingthus motivated to develop highly secure IDS to detect attacks.

2. LITERATURE REVIEW

The algorithms like DES, Triple DES, Blowfish are used when encrypted data to be transmitted[16].They provided the data protection, but up to a certain extent. The Protective measure of highly confidential data is on demand in the market. DES algorithm consumes least decryption time [13]. It is a secret key based algorithm which experiences problems like key distribution and key agreement, but provide throughput in less power intake. On the other hand, AES algorithm uses less memory usage. Cryptographic methods do not hide the secret data [14]. On the other hand, data can be protected by using information hiding techniques. Information hiding techniques embeds the data into cover objects like texts, images, audios, videos. For more security, cryptographic techniques can be applied to an information hiding scheme to encrypt the private data. Steganography can be used to increase chances to hide the data so that the intruders are not able to get the data as it will be hidden behind the image [12].The previous method is made of image encryption, data embedding and data extraction/image recovery phases. The sender encrypts theoriginalimage using an encryption key to produce an encrypted image. Afterward, the data hider compresses theleast significant bits (LSB) of the encrypted images using a data hiding key to create a sparse space to adjust the extra data. At the receiver side, the data embedded in the created space can be easily recovered from the encrypted image containing additional data with the help of da ta hiding key. Since the data embedding only influence the LSB, a decryption with the encryption key can result in an image analogous to the original image. When using both of the encryption and data-hiding keys, the embedded additional data can be extracted and the original image can be perfectly restored by taking advantage of the spatial correlation in natural image. If the lossless compression approx. ach is used for the encrypted image containing embedded data, the additional data can be even now also extracted and the original content of the encrypted image that contains embedded data. On the other hand, the lossy compression method in well-matched with encrypted image producedby pixel permutation is not suitable here since the encryption is done by bit- XOR operating.

A. Image Encryption: The original image in uncompressed design and each pixel with gray value coming under [0,255], denote d by 8 bits. In encryption stage, the XOR results of the original bits and pseudo-random bits are calculated.

B. Data Embedding: In the data embedding stage, some parameters are embedded into a small number of encrypted pixels and the LSB of the other encrypted pixel are compressed to create a space for inserting additional data and the original data at the location occupied by the parameters.

C. Data Extraction and Image Recovery: In this stage, the three cases are taken into account that a receiver has only the data-hiding key, only encryption key, and both the data hiding and encryption keys, respectively. THE first reversible data embedding scheme was put forwarded in Barton, 1997. The algorithm to achieve the reversibility encounters the underflow and overflow problem. The majority of the work on reversible data hiding is done on the data embedding/extracting on theplain spatial domain [17]. But in a number of applications, a low-grade associate or a networkadministrator desires to add-onsone additional message like the origin information, image details or authentication data, within the encrypted image even if he does not know the original image content at the side of receiver. Recently, we have observed that there are numerous system which have non separable data hiding in encryptedimage which have so many limitation and compulsion like user is bound to have all keys to get the data, there is less security for the data. This type of systems cannot be taken in to account while transferring confidEntial data. To overcome limitation of previous system other new system proposes the separable and reversible data hiding technique in which data is going to be embedded in normal form as data have high security compare to image also because data have more priority than image. To overcome these problems, we propose the new system separable and reversible encrypted data in image using AES algorithm. AES algorithm provides the best security to the data to be encrypted as it includes various rounds during decryption. Both hardware and software implementations are faster while using the AES algorithm. Using separable reversible data hiding in image, the security can be increased and overhead can be decreased.

D.Existing system: In the previous reversible data hiding technique [10], the image is compressed and that image is encrypted by using the encryption key and the data is embedded into that image by using the data hiding key. At the receiver side receiver first extract that image [11] using the encryption key in order to extractthe data and after that receiver use data hiding key to extract the embedded data. It is not a parallel process and nor a separable process. Eaack uses digital signatures to secure the acknowledgment packets, but this increases the overhead of routing.

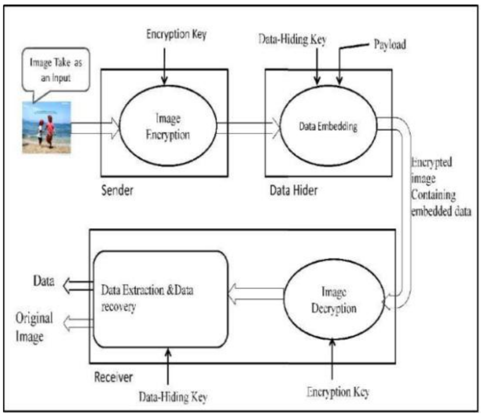

Fig 1: Non-Separable Reversible Data Hiding Using Encrypted Image

LEAST SIGNIFICANT BIT (LSB) METHOD:

In this technique receiver used to embed the data by compressing the LSB bit of encrypted image

DISADVANTAGES OF LSB METHOD:

1. It is efficient for only gray scale images.
2. It has small data embedding capacity**.**

DISADVANTAGES OF EXISTING SYSTEM:

1. If receiver has both data hiding key and the encryption key then only he extract any information from the encrypted imagecontainingadditionaldata.
2. In this system receiver proposes an embeddeddata in an encrypted image by using an irreversible technique of data hiding

3. THE PROPOSED SYSTEM

This survey report consists of implementationon separable reversible data hiding in encrypted image.

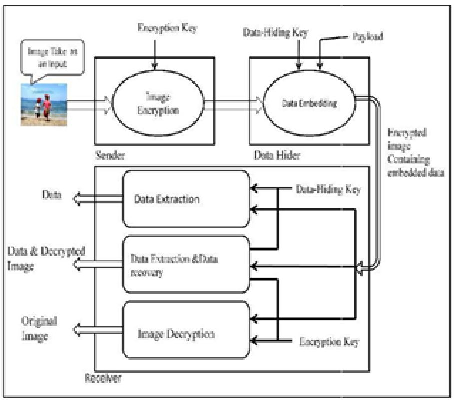

Fig2:SeparableReversibleDataHidingUsingEncryptedImage

In separable reversible data hiding technique, the original image is encrypted using an encryption key and the additional data are fixed into that encrypted image using a data-hiding key. In an encrypted image containing additional data which is hidden behind that image, when the receiver has only the data-hiding key, he is able to extract the additional data though he does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original image, but cannot extract the additional data. If the receiver has both the keys i.e. data-hiding key and the encryption key, then only receiver can extract the additional data and recover the original image without any error. The following algorithms are used for separable reversible data hiding technique in non-encrypted image.

A. Bit plane Complexity System: Various Steganography algorithms like Least Significant Bit (LSB) algorithm, PVD, MBNS and BPCS algorithms. Steganography is the method through which existence of the message can be kept secret. This is accomplished through hiding information in information, thus hiding the existence of the communicated information. This paper gives a brief idea about the image Steganography that make use of BPCS algorithm for hiding the data into image which can be implemented. In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the BPCS method is applied create a space for accommodating the additional data and the original data at the positions occupied by the parameters1. This hop count is initially set to zero, each neighbor that receive beacon packet from base station put it on ID as a source in a packet, increment the hop count and broadcast the beacon in its own neighborhood this beaconing process create the routing tree at the base station. A sensor node shares a unique key with the base station. Since the data is encrypted analysis of the content of the data is not possible. Multiple base techniques perform best routing of packets in the network and help to attain a high data delivery percentage in the presence of more than one Blackholeregion [18].

B. Einstein's algorithm: The Einstein's compression algorithm is a new technique of compression and decompression of images by matrix addition and the possible sequence of the sum. The principle of implementation of a new algorithm is to decrease the complication of algorithms which used for image compression. The most important benefit of this technique is that the compression is highly protected and compressed. This method of compression is a raster type of compression. The image compression is deeming to be Lossless, so it can be used for medical and astronomical images [8]. Simplicity of matrix addition is the most important advantage of the Einstein’s image compression algorithm. The images compressed can be stored in the database with less space. This technique consists of new idea of compression. It does not depend on the previous version of compression. The new variety of the compression technique will be in research for the compression of color images

4. CONCLUSION

In conclusion, using our proposed scheme we were able to encrypt an image using the encryption key and embed data into the image using data-hiding key. Image as well as the data can be retrieved separately without any error. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In general, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. In paper, we have studied a novel scheme for separable reversible da ta hiding using matrix addition approach for color image is proposed, So we can conclude that the Lossless compression of image encrypted by more secure methods will be studied in the future using color images.

References:

[1] XinpengZhang,"Separable Reversible Data Hiding in Encrypted Image”, IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, April 2012.

[2] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," IEEE Trans. Signal Process., vol. 53, no. 10, pp. 3976-3987, Oct. 2005.

[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[4] 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.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted gray scale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097-1102, Apr. 2010.

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

[7] VinitAgham, TareekPattewar, Separable Reversible Data Hiding Technique Base On RGB-LSB Method, IJRAT, Vol.1, No. 3, October 2013, ISSN: 2321-9637

[8] Mohammed Mustaq, Mohammed Mothi, Yasser Arafat, "Einstein s Image Compression Algorithm", Version 1.00, TRIM 7 (2) July -Dec 2011.

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

[10] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Let. vol. 18, no. 4, pp. 255-258, Apr. 2011.

[11] Z. Wang and A. C. Bovik, "A universal image quality index," IEEE Signal Process. Lett. vol. 9, no. 1, pp. 81-84, Jan. 2002.

[12] MazharTayel, HamedShawky, Alaa El-Din Sayed Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data" Feb. 19 22, 2012 ICACT2012.

[13] AkashMandal, Chandra Prakash, Mrs. ArchanaTiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES," IEEE Transom Electrical, Electronics and Computer Science, 2012.

[14] Lokesh Kumar, "Novel Security Scheme for ImageSteganography using Cryptography Technique", Volume
2, Issue 4, April 2012.

[15] Komel Patel, SumitUtareja, Hitesh Gupta, "A Survey of Information Hiding Techniques", Volume 3, Issue 1,Jan 2013, IISN: 2250-2459.

[16] B. Padmavathi, S. RanjithaKumari, "A survey on Performance Analysis of DES, AES and RSA algorithm along with LSB Substitution Technique", Volume 2, Issue 4, April2013,ISSN: 2319-7064.