Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Separable Reversible Data Hiding in Encrypted Image

Ganesh Gunjal
Matoshri College of Engineering & Research Centre Nasik,
Department of Computer Engineering, Savitribai Phule Pune University
Pune, Maharashtra, India

Abstract— recently, different techniques are available for data hiding. When to send some confidential data over insecure channel it is mandatory to embed data in some host or cover media. While sending secure data using cover media it necessary to encrypt as well as compress the cover media after compression embed confidential data. For providing this facility there various encryption/decryption techniques, compression techniques, and data embedding techniques are available. It is also important the data embedding should be reversible in nature. Here we are discussing different data embedding techniques that are reversible in nature by using encrypted image as cover media. In separable reversible data hiding in encrypted image initially the content owner encrypts the original uncompressed image, then the data hider compress the image to create sparse space to accommodate some additional data. At the receiver end, receivers extract the embedded data and recover the cover image without any loss.

Keywords— Separable Reversible Data Hiding, data hiding key, encryption key, Difference expansion.

I. INTRODUCTION

Separable reversible data hiding in encrypted image requires different encryption technique, compression technique and data hiding technique for encrypted image. Data hiding technique is to embed some secret information into some carrier signal by altering the insignificant components for copyright protection. In general cases, the data hiding operation will result in distortion in the host signal. However, such distortion is too small and is unacceptable to some applications, such as military or medical images. In this case secret message is embedded with a reversible manner so that the original image contents can be perfectly restored after extraction of the hidden data. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, [3] Digital watermarking techniques [13,14] and Difference expansion (DE) methods [19].The lossless compression based LSB technique[21],performing lossless compression in order to create a spare space to accommodate additional secret data.

II. NON- SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

Figure 1 shows the design of Non-separable reversible data hiding in encrypted image. Initially, the image undergo encryption phase. Encryption is performed by applying encryption algorithm encryption key (k1) is taken as input. After image encryption secret data is embedded into encrypted image providing data hiding key (k2) as input. On the receiver first image is decrypted by applying encryption key(k1), after image decryption data extraction and image recovery takes place by applying data hiding key(k2). Data extraction is dependent on image decryption.

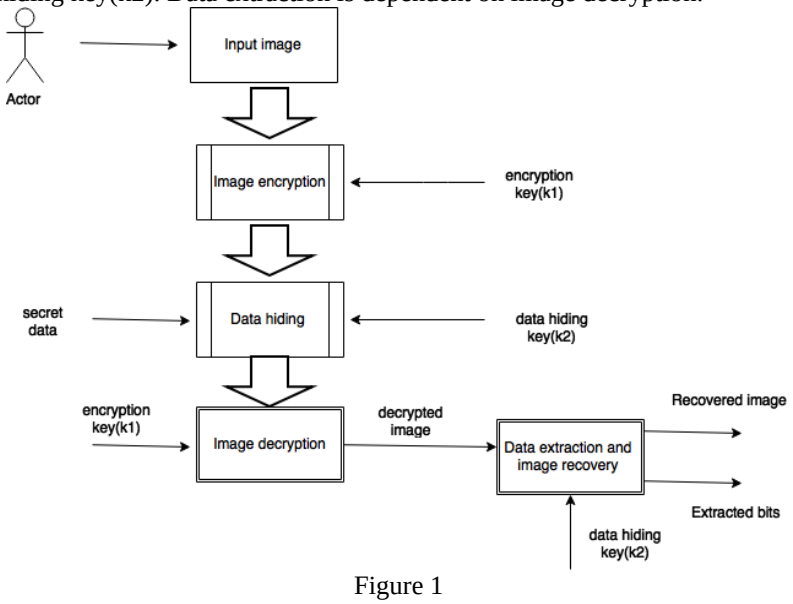

Figure 1

© 2015, IJARCSSE All Rights Reserved

III. SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

Figure 2 show the design of separable reversible data hiding in encrypted image. Initially, the image undergo encryption phase. Encryption is performed by applying encryption algorithm encryption key (k1) is taken as input. After image encryption secret data is embedded into encrypted image providing data hiding key (k2) as input. On the receiver if receiver has data hiding key (k2) then receiver can extract secret data, though receiver unable to decrypt image. If receiver has encryption key (k1), receiver can decrypt image though the image contain small amount of secret data. If receiver has both keys can extract secret data as well as decrypt image without any error.

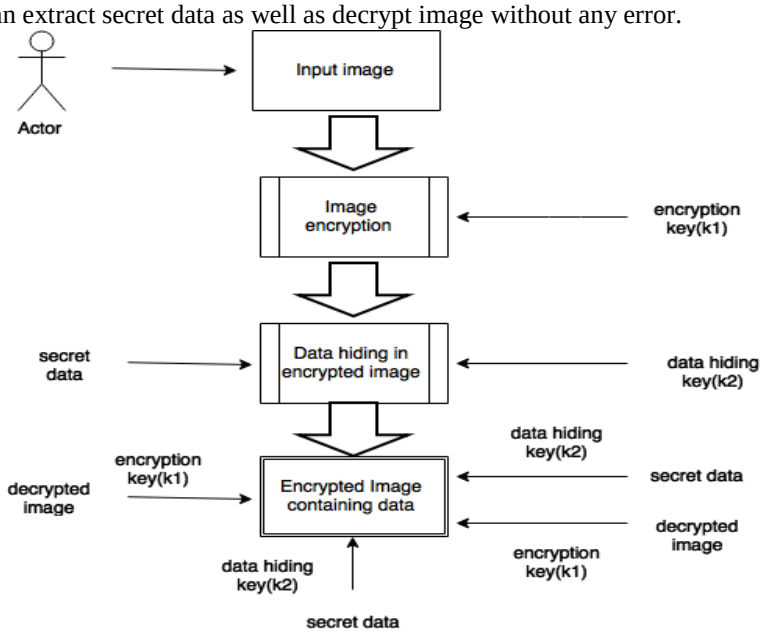

Figure 2

IV. LITERATURE REVIEW

A. Separable Reversible Data Hiding in Encrypted Image: - This technique proposes a novel scheme for separable reversible data hiding in encrypted images [1]. In the first part, a content owner (sender) encrypts the original image i.e. the uncompressed image using key known as an encryption key. Then, the data hider may compress the lower bits i.e. the least significant bits (LSB) of the encrypted image using a new key known as a data-hiding key to create a sparse space to accommodate some additional data. Now with the encrypted image containing the additional data, if a receiver has the data-hiding key, then the receiver can extract the additional data though the receiver does not have an idea about the original image content. If the receiver has encryption key, then the receiver can decrypt the image similar to the original image but receiver cannot extract the additional data. If the receiver has both the keys i.e. data-hiding key and the encryption key, then receiver can extract the additional data and recover the image i.e. the original content of the image without any error by exploiting the spatial correlation.

B. Lossless Compression Method for Encrypted Gray Image: - Wei Liu et.al [3] suggested a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes. In this method resolution progressive compression algorithm, that has been shown to have much better coding efficiency and less computational complexity than existing approaches.Wei Liu and et.al observed that lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources such as images, they are trying to improve the compression efficiency. In this paper researchers proposed a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. Researcher focused on the design and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression. Resolution progressive compression is used for this problem that has much better coding efficiency and less computational complexity than existing approaches.

C. Lossy Compression and Iterative Reconstruction for Encrypted Image: - X. Zhang [10] presented lossy compression method in which 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. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In the encryption phase , only the pixel positions are shuffled and the pixel values are not masked.

© 2015, IJARCSSE All Rights Reserved

D. A Buyer–Seller Watermarking Protocol: - Nasir Memon and Ping Wah Wong [13] worked on a buyer-seller watermarking protocol that is the concept of digital watermarking. In this protocol researchers stated that the seller does not get to know the exact watermarked copy that the buyer receives. Hence the seller cannot create copies of the original content containing the buyer's watermark. However, in case the seller finds an unauthorized copy and can identify the buyer from whom this unauthorized copy has originated and furthermore also prove this fact to a third party by means of dispute resolution protocol. Hence, the buyer cannot claim that an unauthorized copy may have originated from the seller. The watermark embedding protocol is based on public key cryptography and has little overhead in terms of the total data communicated between the buyer and the seller. Nasir Memon and Ping Wong stated the concept of hiding the data in encrypted form of the data. Here seller is doing data (fingerprint/Watermark in this case.) embedding while he does not know the original data content. The data is in the encrypted form.

E. Buyer-seller watermarking protocol based on homomorphic cryptosystem and composite signal: - M.Deng and et.al [14] proposed Buyer-seller watermarking protocol based on homomorphic cryptosystem and composite signal representation in the encrypted domain. Developed the composite signal representation which allows us to decrease both the computational overhead and the large communication bandwidth which are mostly due to the use of homomorphic public-key encryption schemes. Complexity estimates show that the most computational demanding part of the protocol is the encryption of the content and the embedding of the watermark in the encrypted domain. In order to evaluate the feasibility of this part, a practical implementation of an encrypted domain watermark embedding method, based on different watermarking algorithms, has been implemented and tested on different images. The results show that the version using composite signal representation can run in less than two minutes with a performance in terms of robustness almost indistinguishable from that of the corresponding plaintext embedding algorithms.

F. Reversible Data Embedding Using a Difference Expansion: - Jun Tian [19] developed a simple and efficient reversible data-embedding method for digital images in that researcher explored the redundancy in the digital content to achieve reversibility. Both the payload capacity limit and the visual quality of embedded images are best. As a basic requirement, system achieved the policy of quality degradation on the image after data embedding should be low.

Table 1Literature Review

Sr. No	Propose Work	Author	Carrier	Encryption	Data hiding	Description
3	Reversible Data Hiding	NirwanAnsari, Weisu	grayscale image	-	Histogram modification	In this technique Data is pseudo-randomly embedded into histogram of the
5	Reversible Data hiding in encrypted image	XinpengZhang	grayscale image	Pseudo-random permutation	LSB	On encrypted Image lossless LSB compression technique is applied for embedding additional data
6	Lossy Compression And Iterative reconstruction of encrypted image image	XinpengZhang	grayscale image	Pseudo-random permutation	Orthogonal Transform	On receiver side after data Image is recovered iteratively

V. CONCLUSIONS

Surveys on separable reversible data hiding techniques are analyzed. In separable reversible data hiding original image is encrypted after that secret data is embedded, at the receiver end secret data and image are retrieved independently without any loss.

VI. FUTURE SCOPE

In the future, combination of image encryption and data hiding compatible with lossy compression can be implemented. We can use audio, video in case of image as cover for hiding the data.

REFERENCES

[1] Xinpeng Zhang, Separable Reversible Data Hiding in Encrypted Image IEEE Transaction on Information Forensic and Security Vol 7 No.2 April 2012.

© 2015, IJARCSSE All Rights Reserved

[2] Riah Ukur Ginting1, Rocky Yefrenes Dillak "Digital color image encryption using RC4 stream cipher and chaotic logistic map" 978-1-4799-0425-9/13/\$31.00 ©2013 IEEE.

[3] 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.

[4] 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.

[5] P. Moulin and A. Ivanovic, "The zero-rate spread-spectrum watermarking game," IEEE Trans. Signal Process , vol. 51, no. 4, pp.1098–1117. Apr. 2003.

[6] H. S. Malvar and D. A. F. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 898–905, Apr. 2003.

[7] B. Mathon, P. Bas, F. Cayre, and B. Macq, "Optimization of natural watermarking using transportation theory," in Proc. %11th ACM Workshop on Multimedia and Security (MM&Sec'2009), Princeton, NJ, Sep.2009, pp. 33–38.

[8] 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.

[9] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," IEEE Trans. Signal Process., vol. 53, no. 10, pp. 3976–3987, Oct. 2006.

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

[11] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans.Inform. Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.

[12] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[13] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[14] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

[15] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[16] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Processing:\\Image Commun., vol. 26, no. 1, pp. 1–12, 2011.

[17] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proceedings IEEE, vol. 92, no. 6, pp. 918–932, Jun. 2004.

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

[19] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[20] 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.

[21] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no.2, pp. 253–266, Feb. 2005.

© 2015, IJARCSSE All Rights Reserved