DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4830

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

REVERSIBLE DATA-HIDING SCHEMES FOR ENCRYPTED IMAGE: A REVIEW

Anoop Kumar Chaturvedi
Department of Computer Science and Engineering
LNCT, Bhopal (India)

Piyush Kumar Shukla
Department of Computer Science and Engineering
RGPV, Bhopal (India)

Abstract: In this paper, we present a review work on reversible data hiding in images which deals with secure multimedia data and its authenticity. The purpose of preserving content and tampering of image we need to embed some encrypted data image for security and privacy. In the data hiding process, a content is encrypted in the original image using an encryption key. There are entities primarily used in data hiding, image provider (content owner), data hider and receiver they particularly shared a key for encryption. Using some encryption method encrypt sample pixels to non-sample pixels, the data hider who may or may not knows about actual image embed the secret data and then data extraction is done either from encrypted or decrypted domain. Encrypted/hiding key play an important role since if a receiver has the data hiding key, receiver can extract the data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content. In this paper we studies and compared some data hiding scheme.

Keywords: encryption, data hiding, decryption.

1. INTRODUCTION

In recent years, rapid development of data communication in the privacy and security of personal data has attracted researchers to secure and authenticate data communication. There are no guarantees of security or privacy of the stored data will not be accessed by illegal entities, such as the cloud provider itself or attackers. The images now days play a very important role in the field of communication. The images are transferred from place to another in the form of signals, the secret data can be transmitted in the from images, where the secret data will be encrypted in another image with the help of secret key that is provided to together the sender as well as receiver. The customer are much worried about the security of personal data, surveys show that 88% consumers are troubled about the privacy of their data [1]. Under this situation data hiding process in multimedia data is used to maintain the confidentiality in communication. For, confidentiality service provider embed some data for authentication to an encrypted data for detection of tampering or ownership declaration e.g. patient image in medical field contain information of patient through data hiding [2,3].

An effective and popular means for privacy protection signal processing in the encryption converts the signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that image provider does not trust the processing cloud provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. Instantly, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary message can be can be embed to encrypted image [4-7]. The secret message can be embedded into an image by data hider and message can only be extracted by person who know about encrypted key. In this paper we focus only data hiding in an image. In image based data hiding, an image with embed data is known as stego-image and nornal image is known as cover image. Generally, there are two type of data hiding techniques discussed below:

1. Reversible Data Hiding

The reversible data hiding the cover image is extracted using encryption key and the extraction of the payload by using of data hiding key. Message embed in the image i.e. can be extracted using data hiding key but cannot recover the cover image and using encryption key we can recover the cover image as the original but cannot extract the hidden data. We need both of the keys to extract the original image and embed data. Reversible data hiding has found various important applications in field of military imagery, forensics and medical imagery and law where it has importance to reconstruct the original image without any distortion.

2. Non-Reversible Data Hiding

In non-reversible data hiding technique, the content owner encrypts the image by the encryption key then transfers it to the data hider. The data hider hides additional data into the image using the data hiding key. The main aspect of non-reversible data hiding is different from reversible rata hiding is that, at the receiver point to extract the original data and the cover image, we need both of the keys i.e. encryption key and the data hiding key.

The rest of this paper is summarized as follows: section 2, presents previous work related to reversible data hiding. Section 3, we propose our methodology for reversible data hiding scheme. The conclusion is given in Section 4.

2. PREVIOUS WORK

In the recent years, many researchers worked on reversible data hiding methods. Difference Expansion (DE) [8] is a popular methods in which the difference between two neighbouring pixels is expanded for embedding message bit. The capacity of embedding is increase [9,10] by many improved DE-based reversible data hiding schemes.

Another, method is popular approach is Histogram Modification (HM) method in which the histogram of pixel values of the cover image is utilized by using the distribution of the pixel values in an image. A reversible data hiding scheme by rotating the histogram of the cover image according to a particular circular mapping is proposed [11]. HM method utilizes the zero and peak points of the histogram of the cover image and shifts the pixel values to embed data bits into the host image. Some, recent techniques are developed to increasing embedding capacity based on prediction error expansion [12-15] and optimal value transfer matrix to improve embedding capacity [16]. An important scenario of reversible data hiding is that the data hider and service provider are not the same party, and the data hider do not know about the cover image.

Some recent reversible data hiding schemes in encrypted images are proposed in [17-19]. Generally, these schemes can be divided into three categories of reversible data hiding methods for encrypted images, i.e. methods by vacating room after encrypting images [20], methods by reserving room before encrypting images [21], and methods based on homomorphic encryption [22]. These methods are reversible data hiding schemes for encrypted uncompressed images and they cannot be directly applied to compressed images.

Different from above schemes, in [23] a novel method for reversible data hiding in cover images based on interpolation. Before encryption and data embedding, an interpolation method is used to generate error. Select same sample pixels, which are sampled to form the low resolution image, are encrypted using a benchmark stream cipher. Hiding data can be embed in the encrypted image by interpolation method. Interpolation techniques achieve complete reversibility, i.e., no errors occur in data extraction and image recovery. Also, it can be applied to two different application scenarios by extracting the hidden data either from the encrypted image or from the decrypted image.

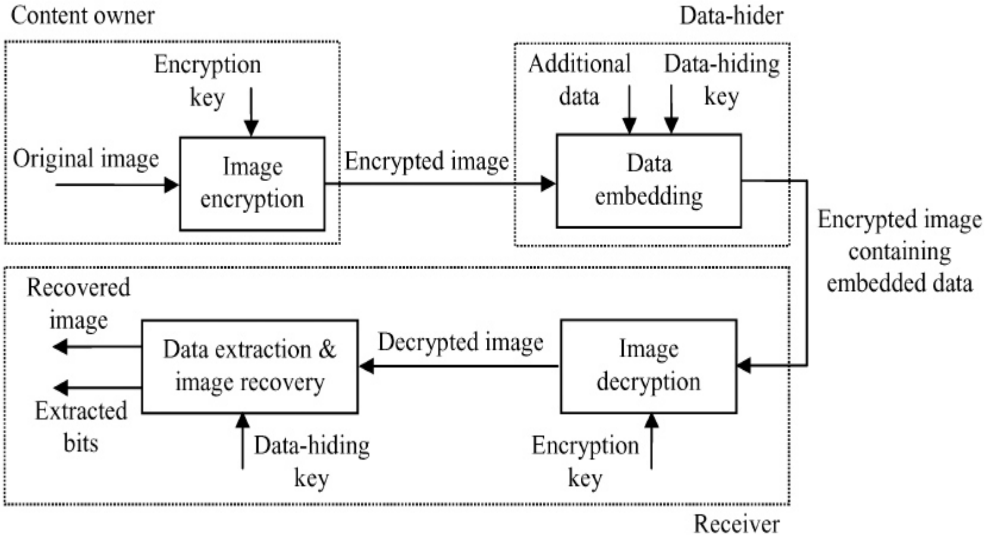

Figure 1: Sketch diagram of reversible data-hiding in cover image

Table 1:The Experimental comparisons of some important methods for reversible data hiding is shown in

Name of Image	Hong et al. [24]		Zhang [25]		Zhang [26]		Chen et al. [27]	
	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR
Lena	0.005	38.08	0.005	38.08	0.035	37.96	0.500	39.38
Aeroplane	0.001	38.33	0.001	38.30	0.031	37.98	0.500	39.84
Pepper	0.005	38.05	0.005	38.05	0.026	37.91	0.500	39.83
sailboat	0.006	37.97	0.003	37.90	0.017	37.95	0.500	39.85
Boat	0.001	37.93	0.004	37.93	0.020	37.93	0.500	39.81
Baboon	0.004	38.37	0.001	38.18	0.008	37.90	0.500	39.84
Avg.	0.004	38.12	0.003	38.08	0.023	37.94	0.500	39.83

3. PROPOSED METHODOLOGY

In this section, we proposed a technique for reversible data hiding in encrypted using data hiding key and encrypted key. Proposed technique of a specialized reversible data hiding in encrypted image is summarized in following phases:

(i). Data Embedding Phase

The image provider embed the data into the cover and encrypts it using encryption key. At the receiver receives it and decrypt it using the key and extracts the data to recovers original image. Data hiding technique along with data extraction and image recovery is described below.

(ii) In an image a pixel is related with its neighbouring pixels, using this relation any pixel can be predicted from a its neighbour pixels. So we need to find the technique to deduce this relation.

(iii) At receiver side, decrypt the encrypted image by applying pixel permutation method.

(iv) Now receiver are able to extract hidden data from decrypted image. the recipient extracts message bits from the decrypted stego-image by scanning the image in the same order as during the embedding.

The procedure of proposed methodology is given below:

3.1. Let three important entity as cover image, data hider and data receiver for encrypted image There are three entities, image provider P, data hider H, and receiver R, in an EIRDH scheme. A valid EIDRH scheme is composed of the following algorithms:

1. First select a cover image and a encrypted key to encrypt the image.
2. Select appropriate data which you want to hide in encrypted image using data hider key. Embedding secret message to encrypted image and returns an encrypted image with the embedded message.
3. If receiver receives image and have decrypted key as input.
4. Extracting the cover image and secret message using received image and data hider key and encrypted key.
6. This algorithm by using received image, taking secret message and the key as input, and then returns the hided message.

4. CONCLUSION

In this paper, we presents a short and simple review about reversible data hiding techniques and their comparison. Also, we shown that how researchers use to improve the capacity of secret message to hide and quality of stego-image. Researchers have been developed different techniques like an improved reversible data hiding in encrypted images, Separable reversible data hiding in encrypted image and Encrypted signal-based reversible data hiding with public key cryptosystem. After studying the literature we came to the points that reversible data hiding method can make more efficient using histogram modification combination with chaotic map. The proposed methodology in this paper can be apply to gray scale images with different hiding capacity and stego-images.

REFERENCES:

[1]. L. Zhou, V. Varadharajan, M. Hitchens, Achieving secure role-based access control on encrypted data in cloud storage, IEEE Trans. Inf. Forensics Secur. vol. 8, no.12, pp.1947–1960, 2013.

[2]. H. Wang, S. Wang, Cyber warfare-steganography vs. steganalysis, Commun. ACM, vol. 47, no. 10, pp. 76–82, 2004.

[3]. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding-a survey, Proc. IEEE, vol. 87, no. 7, pp.1062–1078, 1999.

[4]. J. Fridrich, D. Soukal, Matrix embedding for large payloads, IEEE Trans. Inf. Secur. Forensics, vol. 1, no. 3, pp. 390–394, 2006.

[5]. C. Munuera, Steganography and error-correcting codes, Signal Process. vol. 87, no. 6, pp. 1528–1533, 2007.

[6]. J. Mielikainen, LSB matching revisited, IEEE Signal Process. Lett. vol. 13, no. 5, pp. 285–287, 2006.

[7]. X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Commun. Lett. vol. 10, no. 11, pp. 781–783, 2006.

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

[9]. Y. Hu, H.-K. Lee, K. Chen, J. Li, Difference expansion based reversible data hiding using two embedding directions, IEEE Trans. Multimedia vol. 10, no. 8, pp. 1500–1512, 2008.

[10]. H.J. Kim, V. Sachnev, Y.Q. Shi, J. Nam, H.G. Choo, A novel difference expansion transform for reversible data embedding, IEEE Trans. Inf. Forensics Secur. vol. 3, no. 3, pp. 456–465, 2008.

[11]. C. Vleeschouwer, J.-F. Delaigle, B. Macq, Circular interpretation of bijective transformations in lossless watermarking for media asset management, IEEE Trans. Multimed. vol. 5, no. 1, pp. 97–105, 2003.

[12]. X. Cao, L. Du, X. Wei, D. Meng, X. Guo, High capacity reversible data hiding in encrypted images by patch-level sparse representation, IEEE Trans. Cybern. vol. 46, no. 5, pp. 1132–1143, 2016.

[13]. V. Sachnev, H.J. Kim, J. Nam, S. Suresh, Y.Q. Shi, Reversible watermarking algorithm using sorting and prediction, IEEE Trans. Circuits Syst. Video Technol. vol. 19, no. 7, pp. 989–999, 2009.

[14]. D.M. Thodi, J.J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process. vol. 16, no. 3, pp. 721–730, 2007.

[15]. X. Li, W. Zhang, X. Gui, B. Yang, Efficient reversible data hiding based on multiple histograms modification, IEEE Trans. Inf. Forensics Secur. vol. 10, no. 9, pp. 2016–2027, 2015.

[16]. X. Zhang, Reversible data hiding with optimal value transfer, IEEE Trans. Multimed. vol. 15, no. 2, pp. 316–325, 2013.

[17]. C. Qin, X. Zhang, Effective reversible data hidiing in encrypted image with privacy protectioin for image content, J. Vis. Commun. Image Represent. vol. 31, pp. 154–164, 2015.

[18]. Y.-C. Chen, C.-W. Shiu, G. Horng, Encrypted signal-based reversible data hiding with public key cryptosystem, J. Vis. Commun. Image Represent. vol. 25, pp. 1164–1170, 2014.

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

[20]. C. Qin, X. Zhang, Effective reversible data hidiing in encrypted image with privacy protectioin for image content, J. Vis. Commun. Image Represent. vol. 31, pp. 154–164, 2015.

[21]. K. Ma, W. Zhang, N. Yu, F. Li, Reversible data hiding in encrypted image by reserving room before encryption, IEEE Trans. Inf. Forensics Secur. vol. 8, no. 3, pp. 553–562, 2013.

[22]. Y.-C. Chen, C.-W. Shiu, G. Horng, Encrypted signal-based reversible data hiding with public key cryptosystem, J. Vis. Commun. Image Represent. vol. 25, pp. 1164–1170, 2014.

[23]. M. Takayama, K. Tanaka, K. Takagi, Y. Nakajima, A scalable video scrambling method in mpeg compressed domain, in: Proceedings of the International Symposium on Communications, Control and Signal Processing, 2008, pp. 1035–1040.

[24]. W. Hong, T.S. Chen, H.Y. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Process. Lett. vol. 19, no. 4, pp. 199–202, 2011.

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

[26]. X. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. Inf. Forensics Secur. vol. 7, no. 2, pp. 826–832, 2012.

[27]. Yu-Chi Chen, C. W. Shiu, G. Horng, Encrypted signal-based reversible data hiding with public key cryptosystem, J. Vis. Commun. Image R. vol. 25, pp. 1164–1170, 2014.