

A Survey on Reversible Data Hiding

Amita Anil Ghadyalji¹, Dr. Prashant V. Ingole²

¹Department of Electronics and Telecommunication, SGBAU Amravati, G.H. Raisoni College of engineering and Management, Amravati (M.S.) India

²Professor, Department of Electronics and Telecommunication, SGBAU Amravati, G.H. Raisoni College of engineering and Management, Amravati (M.S.) India

Abstract: The conventional reversible data hiding (RDH) algorithms pursue high Peak-Signal-to-Noise Ratio (PSNR) at certain amount of embedding bits. But now-a-days, improvement of image visual quality is more important than keeping high PSNR. Based on this viewpoint, a novel RDH scheme, utilizing contrast enhancement to replace the PSNR is presented with the help of integer wavelet transform (IWT). To overcome the problem of over-enhancing of image, again a new RDH scheme is proposed using the controlled contrast enhancement (CCE) and integer wavelet transform (IWT). The proposed scheme will analyze various types of wavelet transform that are best suitable in given situation and will also have large embedding capacity while maintaining satisfactory visual perception with improved security.

Keywords: Encryption, Decryption, Reversible Data hiding, Data Recovery, Wavelet Transform, Contrast Enhancement.

1. Introduction

Data hiding is applied extensively to the fields of ownership protection, fingerprinting, authentication and secret communication. The most classical data hiding leads to permanent distortion. But newly proposed Reversible Data Hiding technique can not only extract the embedded bits, but also restore the original cover image without any error. The data may be any text related to the image such as authentication data or author information. In some high-precision applications such as medical, military and remote sensing; it is highly desired that the original image should be perfectly recovered after data extraction. A data hiding technique satisfying this requirement is known as Reversible Data hiding. They are also called as invertible, lossless or distortion-free data hiding.

into the encrypted image using the data hiding key. Data Hiding is the technique by which some data is hidden into a cover media. At receiver side, the original image must be extracted from the hidden encrypted format. The receiver must have both the keys for getting original image as well as the information or data.

In above two figures, the overview of reversible data hiding is shown. In this scheme the content owner encrypt and embed the data at sender side and at receiver side the receiver provides the encryption key to decrypt the image first and then data hiding key to extract the hidden data from the image. This is the sequential process to unhide the data and recover the image.

2. Literature Review

A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. In practical aspect, many RDH techniques have emerged in recent years.

Zhang [1] suggests a completely unique methodology for divisible reversible knowledge activity. Here content owner initially encrypts the initial uncompressed image by writing secret key to provide associate encrypted image. Then, the knowledge-hider compresses the smallest amount important bits (LSB) of the encrypted image employing a data-hiding key to form a thin house to accommodate the extra data. At the receiver facet, the information embedded within the created house will be simply retrieved from the encrypted image containing extra data in line with the data-hiding key. Since the info embedding solely affects the LSB, a decipherment with the secret writing key may result in a picture similar to the original version. Once it is done, the embedded extra knowledge will be successfully extracted and also the original image will be recovered by exploiting the abstraction correlation in natural image. But the only drawback of this method was inefficient Data compression. A novel reversible data hiding scheme[2] for encrypted

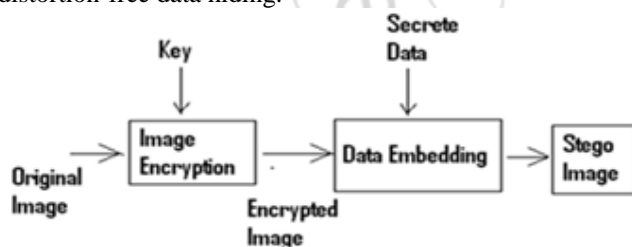


Figure 1: Transmission of Encrypted Data

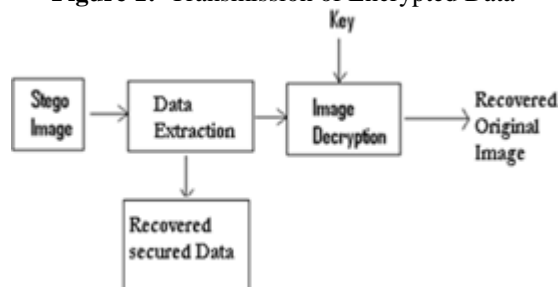


Figure 2: Reception of Original Image

In Reversible Data Hiding technique, the original image is obtained at the receiver side after encryption of data with the help of some secret keys. For this purpose, the content owner first encrypts the image using encryption key. Next to encryption, the data hiding algorithm then hides some data

image was proposed. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB-stageanalytic methods.

A novel scheme to reversibly hide data into encrypted grayscale image [3] was proposed in a separable manner. During the first phase, the content owner encrypts the image by permuting the pixels using the encryption key. The data hider then hides some data into the encrypted image by histogram modification based data hiding, making use of data hiding key. At the receiver side, if the receiver has both keys, S/he may first extract the data using data hiding key and then decrypt the image using encryption key. A method for contrast enhancement[4] was then proposed. This method was a combination of two basic contrast enhancement methods i.e. transform and histogram. Atfirst we apply Non-subsampled Contourlet Transform (NSCT) onthe source image, then NSCT coefficients are mapped to fuzzy domain and modified by a mapping function in fuzzy domain. After transforming the modified values from fuzzy domain into frequency domain, the enhanced image isreconstructed from the modified NSCT coefficients by inverse NSCT. Finally, histogram of the image is equalized by ContrastLimited Adaptive Histogram Equalization (CLAHE).Experimental results and objective evaluations show that this method achieves better contrast enhancement than both NSCT and HE methods. Vasiliy Sachnev, Hyoung Joong Kim, Jeho Nam Sundaram Suresh, and Yun Qing Shi introduced a Reversible Watermarking Algorithm Using Sorting and Prediction[5]. Here sorted prediction errors and reduced size location map allow embedding more data into the image with less distortion. Also sorting technique is used

to record the prediction errors based on magnitude of its local variance. Bhaskara Reddy has suggested an Effective Algorithm of Encryption and Decryption of Images [6] using Random Number Generation Technique and Huffman coding. They considered an image reads its pixels and convert it into pixels matrix of order as height and width of the image. These pixels were replaced into some fixed numbers and key was generated using random generation technique to encrypt an image.The decryption is reverse process of encryption. Hence the proposed method provides a high security for an image with minimum memory usage. The main steps in the encryption algorithm are
 Step 1. Replace each pixel by fixed number values.
 Step 2 .Generate the secrete key by using random generation technique
 Step 3. Huffman Coding. The steps in image decryption are reverse of encryption algorithm.

Contrast limited adaptive histogram equalization (CLAHE) [7] produced an effective algorithm to enhance the local details of an image. However, it faces the contrast overstretching and noise enhancement problems. To solve these problems, Huang Lidong, ZhaoWei, Wang Jun, Sun Zebin presented a novel image enhancement method, named CLAHE-discrete wavelet transform (DWT), which combines the CLAHE with DWT.Nosrati and some other people [8] presented a new technique for data hiding. In this main technique as the principles of RDH were talked. Pair-wise logical computation data hiding technique (PWLC) and Data hiding by template ranking with symmetrical Central pixels(DHTC) technique were used.

3. Proposed Work

Here, a new data hiding technique is proposed which can not only control the over-stretching of image but will also prevent the overflow/underflow while maintaining satisfactory visual perception.

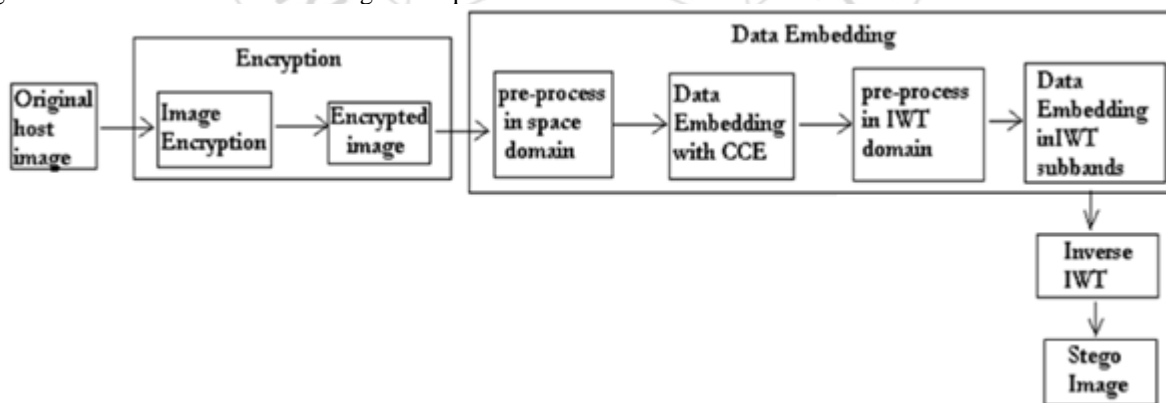


Figure 3: Encryption of Data at Transmitter

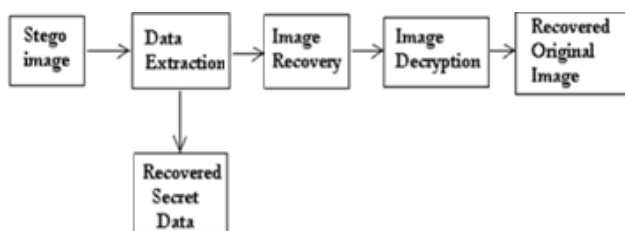


Figure 4: Decryption of data at receiver

The proposed block diagrams for encryption of data at transmitter and decryption of data at receiver are shown in figures 3 and 4 above. There are two main parts in the message embedding process, including data embedding with CCE in spatial domain more data embedding in IWT domain. The encrypted image will be obtained by performing encryption operation on the original host image. Then the data will be embedded with this encrypted image to improve the security of data and the stego image will be

obtained by applying inverse IWT to embedded data. This stego image with embedded data is then transmitted to other side with improved security. The data extraction and image recovery are the reverse procedure of data embedding

4. Conclusion

Based on the RDH algorithm, a new RDH scheme utilizing controlled contrast enhancement and embedding more data into the detail sub band coefficients using different wavelet transform is proposed. It avoids severe distortion as data embedding rate is high. Furthermore, the proposed scheme can embed significantly larger amount of data and achieve better visual quality from human vision point of view. Hence we will consider the wavelet transform which will give the better results and will prevent the overflow/underflow.

References

- [1] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.
- [2] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image", in *IEEE signal processing letters*, VOL. 18, NO. 4, pp 255-258, April 2011
- [3] Rintu Jose, Gincy Abraham, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance", in *International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013)*.
- [4] A. M. Reza, "Realization of the Contrast Limited Adaptive Histogram Equalization (CLAHE) for Real-Time Image Enhancement", *Journal of VLSI Signal Processing* 38, Kluwer Academic Publishers. Manufactured in The Netherlands, 2004, pp.35-44
- [5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009
- [6] Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti, Mr. T. Sri Harish Reddy, Dr. S. Kiran "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" Hema Suresh Yaragunti et al, *Int. J. Computer Technology & Applications*, Vol 4 (6), 883-891
- [7] Huang Lidong, Zhao Wei, Wang Jun, Sun Zebin, School of Electronic and Information Engineering, Beihang University, 100191, People's Republic of China, *IET Image Process.*, 2015, Vol. 9, Iss. 10, pp. 908–915
- [8] Nosrati * Ronak Karimi Mehdi Hariri, "Reversible Data Hiding: Principles, Techniques, and Recent Studies". *World Applied Programming*, Vol (2), Issue (5), May 2012. 349-353 ISSN: 2222- 2510 ©2011 WAP journal.
- [9] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," *Lecture Notes in Computer Science*, vol. 3304, pp. 115–124, 2005
- [10] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 873–882, 2011

process. Hence we will get the recovered original image at receiver side securely and will try to prevent the overflow/underflow.

- [11] P. Basant, T. Furon, "A new measure of watermarking security: The effective key length," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 1306–1317, 2013.
- [12] G. Coatrieux, W. Pan, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 111–120, 2013
- [13] B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, "Pairwise prediction-Error expansion for efficient reversible data hiding," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5010–5021, 2013
- [14] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 507–518, 2015