A Reversible Data Hiding with Contrast Improvement of Digital Image

Reshma Pathan[1], Ankur Shrivastav[2]
[1]*Student, Nuva College of Engineering & Technology, Kalmeshwar,Nagpur , India*
[2]*Assistant Professor, Nuva College of Engineering & Technology, Kalmeshwar,Nagpur , India*

***Abstract*- Embedding capacity, but few consider keeping or improving visual image quality. A new RDH method with contrast enhancement (RDH-CE) is, by pair-wisely expanding the histogram to the lower end to upper end. RDH-CE is especially valuable in exploiting the details of poorly illustrated images for which the visibility of image details is more important than just keeping PSNR high. However, obvious visual image distortion appears when embedding level gets high, and embedding capacity is relatively low when embedding level is small. In this paper, Wu et al.'s work is improved from four perspectives, namely image contrast enhancement, visual distortion reduction, encryption/decryption of image, and embedding capacity increment. The image contrast is improved by making the histogram shifting process adaptive to the histogram distribution characteristics, the image visual distortion is reduced by cutting off half the modification range of pixels induced in histogram pre-shifting, and the embedding capacity is increased by exploiting the pixel value ordering technique at the early stage of data embedment. A simulation result proves that the proposed work is effective in improving image contrast, reducing visual image distortion, and increasing embedding capacity. The proposed system obtained a peak signal-to-noise ratio (PSNR) of about 1–2 dB greater than the original image.**

***Index Terms*- Reversible Data Hiding (RDH), Embedding, PSNR.**

I. INTRODUCTION

Today, the demand of internet has made the transmission of digital media much easier and faster. Open nature of internet, risks of illegitimate accessing and unauthorized tempering with transmitted data is increased day by day. Protection of secret information from unauthorized users in a public network has become an important issue. Data hiding is one of the most demanding techniques to protect the security of digital media [1-5].

RDH is to embed a piece of information into a host signal to generate the marked one, from which the original signal can be exactly recovered after extracting the embedded data. The technique of RDH is useful in some sensitive applications where no permanent change is allowed on the host signal. In the literature, most of the proposed algorithms are for digital images to embed invisible data (e.g. [1]–[8]) or a visible watermark (e.g. [9]). To evaluate the performance of a RDH algorithm, the hiding rate and the marked image quality are important metrics. There exists a trade-off between them because increasing the hiding rate often causes more distortion in image content.

To measure the distortion, the peak signal-to-noise ratio (PSNR) value of the marked image is often calculated. Generally speaking, direct modification of image histogram [2] provides less embedding capacity. In contrast, the more recent algorithms (e.g. [5]–[8]) manipulate the more centrally distributed prediction errors by exploiting the correlations between neighboring pixels so that less distortion is caused by data hiding. Although the PSNR of a marked image generated with a prediction error based algorithm is kept high, the visual quality can hardly be improved because more or less distortion has been introduced by the embedding operations. For the images acquired with poor illumination, improving the visual quality is more important than keeping the PSNR value high. Moreover, contrast enhancement of medical or satellite images are desired to show the details for visual inspection. Although the PSNR value of the enhanced image is often low, the visibility of image details has been improved. To our best knowledge, there is no existing RDH algorithm that performs the task of contrast enhancement so as to improve the visual quality of host images. So in this study, we aim at inventing a new RDH algorithm

to achieve the property of contrast enhancement instead of just keeping the PSNR value high.

To perform data embedding and contrast enhancement at the same time, the proposed algorithm is performed by modifying the histogram of pixel values. Firstly, the two peaks (i.e. the highest two bins) in the histogram are found out. The bins between the peaks are unchanged while the outer bins are shifted outward so that each of the two peaks can be split into two adjacent bins. To increase the embedding capacity, the highest two bins in the modified histogram can be further chosen to be split, and so on until satisfactory contrast enhancement effect is achieved. To avoid the overflows and underflows due to histogram modification, the bounding pixel values are pre-processed and a location map is generated to memorize their locations. For the recovery of the original image, the location map is embedded into the host image, together with the message bits and other side information. So, the blind data extraction and complete recovery of the original image are both enabled. The proposed algorithm was applied to two set of images to demonstrate its efficiency [10-12]. To our best knowledge, it is the first algorithm that achieves image contrast enhancement by RDH. Furthermore, the evaluation results show that the visual quality can be preserved after a considerable amount of message bits have been embedded into the contrast-enhanced images, even better than three specific MATLAB functions used for image contrast enhancement.

The rest of this paper is organized as follows. Section II review the literature about RDH algorithm, Section III presents the details of the proposed RDH algorithm featured by contrast enhancement. The simulation results are given in Section IV. Finally, a conclusion is drawn in Section V.

II.RELATED WORK

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest.

In theoretical aspect, Kalker and Willems [1] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memoryless covers and proposed a recursive code construction which, however, does not approach the bound. Zhang et al. [2], [3] improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the equivalence between data compression and RDH for binary covers. In practical aspect, many RDH techniques have emerged in recent years. Fridrich et al. [4] constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE) [5], in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS) [6], in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods [7]–[11] usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance. With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images.

In [13], Hwang et al. advocated a reputation-based trust-management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data coloring technique based on encrypted data is preferred. Suppose a medical image database is stored in a data center, and a server in the data center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage the image or verify its

integrity without having the knowledge of the original content, and thus the patient's privacy is protected. On the other hand, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible manner for the purpose of further diagnosing. Some attempts on RDH in encrypted images have been made.

In [14], Zhang divided the encrypted image into several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image. Hong et al. [12] ameliorated Zhang's method at the decoder side by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve much lower error rate. These two methods mentioned above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction.

III. PROPOSED MEHODOLOGY

Currently available data hiding techniques do not pay much attention on stego-object (hidden information in original object) with respect to its originality of cover (original) object. Both cover-objects and stego-objects are drifted in context of (quality measure in image) peak signal to noise ratio (PSNR) and mean square error (MSE) aspects. This paper proposed a data hiding method around the edge boundary of an object with high PSNR. The experimental results show very high rate of PSNR. Proposed scheme is targeted for low rate of hidden data but with high PSNR. We have proposed an edge boundary based information hiding method with high PSNR and with high perceptual transparency as well as comparison with original cover image. Through experimental results proposed technique has high perceptual transparency with low computational complexity. Stego-image can further be used as an original image for application (segmentation of objects, feature extraction of objects). Its information hiding capacity can easily be increased depending on computed threshold. Thresholds may vary depending on the image visual characteristics to consider its high PSNR. Moreover, extraction of the secret information is independent of original cover image.

A. Reversible Image Data Hiding with Contrast Enhancement

The procedure of the proposed algorithm [17] is illustrated in figure 1. Given that totally pairs of histogram bins are to be split for data embedding, the embedding procedure includes the following steps:

- Pre-process: The pixels in the range of [0,L-1] and [256-L, 255] are processed excluding the first 16 pixels in the bottom row. A location map is generated to record the locations of those pixels and compressed by the JBIG2 standard [15] to reduce its length.
- The image histogram is calculated without counting the first 16 pixels in the bottom row.
- Embedding: The two peaks (i.e. the highest two bins) in the histogram are split for data embedding by applying equation to every pixel counted in the histogram. Then the two peaks in the modified histogram are chosen to be split, and so on until pairs are split. The bit stream of the compressed location map is embedded before the message bits (binary values). The value of the length of the compressed location map, the LSBs collected from the 16 excluded pixels, and the previous peak values are embedded with the last two peaks to be split.
- The lastly split peak values are used to replace the LSBs of the 16 excluded pixels to form the marked Image

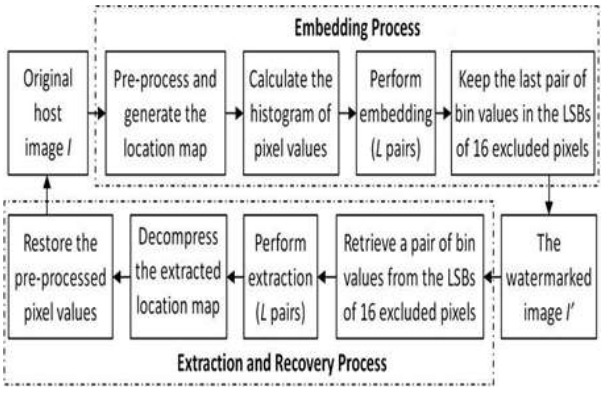

Figure 1: Procedure of the proposed RDH algorithm

The extraction and recovery process include the following steps:

- The LSBs of the 16 excluded pixels are retrieved so that the values of the last two split peaks are known.

- The data embedded with the last two split peaks are extracted, so that the value of, the length of the compressed location map, the original LSBs of 16 excluded pixels, and the previously split peak values are known. Then the recovery operations are carried out by processing all pixels except the 16 excluded ones with the process of extraction and recovery is repeated until all of the split peaks are restored and the data embedded with them are extracted.
- The compressed location map is obtained from the extracted binary values and decompressed to the original size.
- With the decompressed map, those pixels modified in preprocess are identified. Among them, a pixel value is subtracted by if it is less than 128, or increased by otherwise. To comply with this rule, the maximum value of is 64 to avoid ambiguity. At last, the original image is recovered by writing back the original LSBs of 16 excluded pixels.

IV. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images

REFERENCES

[1] Hao-Tian Wu, Jean-Luc Dugelay, and Yun-Qing Shi," Reversible Image Data Hiding with Contrast Enhancement", IEEE SIGNAL PROCESSING LETTERS, VOL. 22, NO. 1, JANUARY 2015.

[2] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[3] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011),LNCS 6958, 2011, pp. 255–269, Springer-Verlag.

[4] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[5] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securit and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

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

[7] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354– 362, Mar. 2006.

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

[9] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[10] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.

[11] L. Luo et al., "Reversible imagewatermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[12] 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.

[13] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[14] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[15] 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.