International Journal of Research in Advent Technology, Vol.4, No.6, June 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Increasing Robustness in Reversible Image Data Hiding with Contrast Enhancement by Homomorphic Encryption

Rasika P. Kulkarni[1], Archana S. Vaidya[2]
Department of Computer Engineering[1, 2]G. E. S., R. H. Sapat College of Engineering, Management & Research, Savitribai Phule Pune University,Nashik, India.[1, 2]
Student[1], Professor[2]
Email: rasikool10@gmail.com[1] , archana.s.vaidya@gmail.com[2]

Abstract-Reversible data hiding (RDH) is also referred as invertible data hiding, RDH is to insert a piece of data into a host picture to generate the marked one, from which the original picture can be exactly recovered after extracting the embedded data. The RDH algorithm with contrast enhancement enhances the contrast of a host image to enhance its visual quality, by avoiding to keep the PSNR esteem high. The topmost two receptacles in the histogram are selected for data embedding so that by repeating the process, histogram equalization can be performed .The side data is inserted along with the message bits into the original image, So it is completely recoverable. For improving the robustness, Homomorphic encryption is utilized as a contribution in the existing system which additionally gives security to avoid the cipher-text attacks so that it can be applicable to medical images.

Index Terms- Contrast Enhancement, Histogram Modification, Location map, Reversible Data Hiding, Visual Quality, Homomorphic Encryption.

1. INTRODUCTION

In the Reversible information hiding the orig-inal image can be perfectly recovered after extracting the embedded data, also referred as lossless data hiding, RDH is to insert a piece of data into a host image to generate the stamped one. The method of RDH is utilized in some touchy applications where no perpetual change is permitted on the host signal. In the writing overview, most of the proposed calculations are for digital images to insert invisible data or a visible watermark. The hiding rate and the marked image quality are important mea-surements, to improve the performance of a RDH algorithm. If hiding rate is increased, it often causes more distortion in image content, as there exists a trade-off relation between them. We usually calculate the peak signal-to-noise ratio (PSNR) value of the marked image to measure the distortion. Less distortion is caused by data hiding by exploiting the cor-relations between neighboring pixels.Contrast enhancement of medical or satellite images is expected, to show the details for visual inspection.

By avoiding just to maintain the PSNR es-teem high, to accomplish the property of con-trast enhancement, in this study, our aim is to invent a new RDH algorithm.Here, data embedding and contrast enhancement is per-formed at the same time by modifying the histogram of pixel values. Firstly, the highest two tops in the histogram are discoverd. The bins between the peaks are unalterd while the external bins are moved outward therefore each of the two peaks can be split into two adjacent receptacles. The highest two bins in the modified histogram can be chosen again to be split until satisfactory contrast enhancement effect is achieved, till the embedding capacity is increased. The bounding pixel values are pre-handled and a location map is generated for retaining their locations, to avoid the overflows and underflows due to histogram alteration. The location map is inserted into the original picture together with the message bits and other side data to recover the original picture. So blind information extraction and complete recovery of the original picture are both en-abled.

For improving the robustness of algorithm the technique of homomorphic encryption is used. Homomorphic encryption uses secret key and public key for data encryption. Homomor-phic encryption is our contribution which is used for providing the security and improv-ing the robustness of Reversible Image data hiding. Security of data is very important in sensitive fields like medical.When evaluating the security of the image homomorphic en-cryption scheme in [16], we assume that the Paillier cryptosystem is secure.According to the information that is available to the attacker, the attacks can be classified into several types.

- A ciphertext-only attack (COA) is one where the assailant tries to deduce the secret key by only watching the ciphertext.
- A known-plaintext attack (KPA) is one where the attacker has a amount of plaintext and the associated ciphertext.

- A chosen-plaintext attack (CPA) is one where the attacker picks or selects plaintext and is then given the relating ciphertext [16].
- A chosen-ciphertext attack (CCA) is one where the attacker can have access to the de-coder, and thus can chooses ciphertext and obtain the relating plaintext [16].

2. LITERATURE SURVEY

Tian, Jun [1] displayed a novel reversible infor-mation embedding method for digital images. They investigated the repetition in digital im-ages for accomplishing very high embedding limit, and keep the distortion low. Ni, Zhicheng et al. [2] presented a reversible data hiding algorithm, which is able to recuperate the orig-inal picture without any distortion from the stamped picture after the embedded data have been extracted. This method utilizes the zero or the minimum points of the histogram of an image.

Thodi, Dilith M., and Jeffrey J. Rodrguez [3] proposed a histogram moving strategy as an alternative for installing the location map. The proposed approach enhances the distor-tion performance at low embedding limits fur-thermore mitigates the capacity control issues. Coltuc, Dinu, and J-M. Chassery [4] discussed that Reversible contrast mapping (RCM) is a simple integer transform that applies to pairs of pixels. RCM is invertible, for few set of pairs of pixels, even if the least significant bits (LSBs) of the changed pixels are lost.Yang, Ying et al. [5] proposed a reversible (also called lossless, distortion-free) noticeable watermarking proce-dure to fulfill the applications, in which the visible watermark is expected. Sachnev, Vasiliy et al. [6] exhibited a lossless watermarking calculation for images without using a location map in numerous cases. This algorithm utilizes prediction errors to implant information into an image.

Li, Xiaolong et al. [7] proposed to embed 1 or 2 bits into expandable pixel indicated by local complexity. This avoids growing pixels with vast prediction-errors, hense it diminishes embedding impact by decreasing the maxi-mum adjustment to pixel values.Zhang, Xin-peng et al.[8] proposed a novel reversible in-formation hiding plan for encoded image. After encrypting the entire information of an uncom-pressed image by a stream cipher, the extra information can be implanted into the image by changing a little proportion of encrypted information.Fallahpour et al. [9] introduced a highly productive reversible information hid-ing framework. It depends on dividing the im-age into tiles and then moving the histograms of every image tile between its base and gratest frequency. Zhao, Zhenfei et al. [10] approched a reversible information hiding method for common images.Because of the similarity of neighbor pixels values such a large number of contrast between sets of contiguous pixels are near zero.

Zhang, Xinpeng [11] proposed a novel plan for separable reversible information covering in encrypted images. In the primary stage, a content owner encodes the original uncom-pressed image utilizing an encryption key.Wu, Hao-Tian, and Jiwu Huang [12] proposed a reversible information hiding algorithm, in which the efficiency of changing a couple of histogram bins is analyzed.Gao, Ming-Zhi et al. [13] discussed the guideline of picture enhance-ment which is based on expanding the con-trast between neighboring pixels, permitting viewers to visually perceive images with more detail in the textures and edges.Jose, Rintu, and Gincy Abraham [14] proposed a novel plan to reversibly hide information into encrypted grayscale picture in a distinct manner. Payal V. Parmar, Shraddha B. Padhar [15] survey the different algorithms of Homomorphic encryp-tion. Yunyu Li, Jiantao Zhou, and Yuanman Li [16] have investigated the security issue of a recently published image homomorphic encryption strategy with little ciphertext exten-tion.

3. PROPOSED SYSTEM

3.1. *Algorithms*

In the Proposed system , The Reversible Data Hiding algorithm is utilized with contrast enhancement strategy. Homomorphic encryption is used for improving robustness and providing security. We utilized the functions Pre-processing, Histogram calculation, Homomorphic encryption, Embedding, Decoding, Homomorphic decryption, Image recovery. The Proposed architecture is shown in Fig 1.

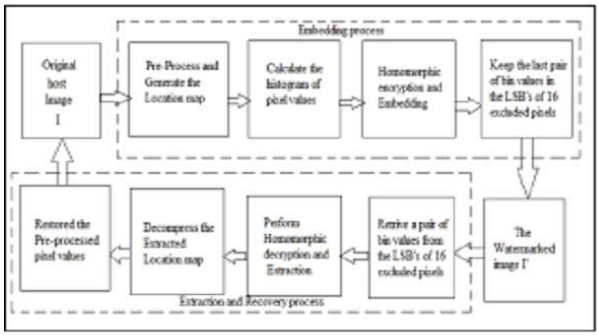

Fig. 1. Proposed System Architecture

(1) Homomorphic encryption algorithm :

Homomorphic encryption is our contribu-tion for providing the robustness and security. Encryption of the plaintext is done by using the homomorphic

algorithm which is shown in TABLE 1.Private and public key is generated in this algorithm for maintaining security of plaintext.Encryption of image is done by us-ing image homomorphic encryption of paillier cryptosystem.The idea of image homomorphic encryption scheme is to first generate a pixel sequence S = (S_0; S_1; :::::; S_K 1) where K is smaller than the number of pixels in the input. let I = I(x,y) be the image to be encrypted, where 0 x; y M1. P([[I]],[[S]]) is used to denote the index map relative to [[S]].

TABLE 1. Homomorphic Algorithm

Start
Step 1: select any two prime numbers say p and q
Step 2: calculate the product of those two prime numbers. Say N = p * q. where p and q being confidential and N is public.
Step 3: select random number x and a root g of GF(p). where g and x are smaller than p.
Step 4: calculate y = gx mod p. use this y for the encryption.
Step 5: encryption will be performed in following two steps: 1. Select random integer number r and apply following homomorphic encryption. E1(M) = (M+r*p) mod N. 2. Select random integer number k, and the encryption algorithms are: Eg(M) = (a,b) = (gk mod p, yk E1(M)mod p)
Step 6: Decrypted algorithm $D_g()isM = b(a^x)^{-1}(modp)$.
End

(2) Embedding Procedure :

The technique of the proposed algorithm is represented in Fig. 1. Given that totally pairs of histogram bins are to be split for data embed-ding, the embedding procedure includes the following steps:

$$i' = \begin{cases} i-1, & for\, i < I_S \\ I_S - b_k, & for\, i = I_S \\ i, & for\, I_S < i < I_R \\ I_R + b_k, & for\, i = I_R \\ i+1, & for\, i > I_R \end{cases} \quad (1)$$

(a) Pre-process: The pixels in the scope of [0,L-1] and [256-L,255] are processed, excluding the initial 16 pixels in the bottom row. A location map is created to record the locations of those pixels and compressed to reduce its length [17].

(b) The information embedded with the last two split peaks are extracted by utilizing Eq. (2) [17] therefore the estimation of the length of the compacted location map, the original LSBs of 16 excluded pixels, and the previously split top values are known. Then the recovery operations are carried out by processing all pixels except the 16 excluded ones with Eq. (3) [17]. The procedure of extraction and recovery is repeated until all of the split tops are restored and the information embedded with them are extracted.

$$b'_k = \begin{cases} 1, & if\, i' = I_S - 1 \\ 0, & if\, i' = I_S \\ 0, & if\, i' = I_R \\ 1, & if\, i' = I_R + 1 \end{cases} \quad (2)$$

(c) The compressed location map is obtained from the extracted binary values and decompressed to the original size.With the decompressed map, those pixels changed 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 uncertainty.Finally, the original image is recovered by composing back the original LSBs of 16 excluded pixels [17].

$$i = \begin{cases} i'+1, & for\, i' < I_S - 1 \\ I_S, & for\, i' = I_S - 1 or\, i' = I_S \\ I_R, & for\, i' = I_R or\, i' = I_R + 1 \\ i'-1, & for\, i' > I_R + 1 \end{cases} \quad (3)$$

4. RESULT AND DISCUSSION

A dataset of 8 USC-SIPI test images with the extent of 512*512 [12] and 24 Kodak test pictures with the span of 768*512 [13] were utilized and changed over into grey-level images. We utilized some standard images and medical images as a test images for testing the visibility of images. The implementation is in the Java language.The Result table 2 shows that the quality of recovered image is maintained and PSNR value is near to 40DB which is better than the existing system [17] even after embedding the encrypted data in the encrypted image.

4.1. *Pre-Processing and Calculation of Histograms values*

In the algorithm, it is required that all pixels counted are inside 0,1,..254,255 . If there is any bounding pixel esteem (0 or 255), histogram moving will cause overflow or underflow.In perticular, the pixel values of 0 and 255 are modified to 1 and 254, respectively.

Table 2. RESULT TABLE

Image Name	Text Size (bytes)	PSNR Value (DB)
Lena	42	44.69
Airplane	53	40.41
Baboon	79	31.01
Barbara	68	36.19
Boat	77	32.00
Peppers	65	35.96
Car1	51	41.44
Space	69	35.13
Flowers	67	33.56
Piano	78	31.79

So that, no overflow or underflow will be created because the possible change of each pixel value is 1. A location map with the similar size as the
original image is created by assigning 1 to the location of a adjusted pixel, and 0 to that of an unaltered one, to remember the pre-processed pixels (including the 16 excluded pixels).

4.2. *Contrast Enhancement*

Both tops in the histogram are split into two neighboring receptacles individually.To expand the hiding rate, the most elevated two bins in the adjusted histogram are again chosen to be split by applying Eq. (1) to all pixels counted in the histogram [17] .The same procedure can be repeated by splitting each of the two peaks into two adjacent bins having similar heights. In this way the histogram equalization effect is achieved. Thus data embedding and contrast enhancement are simultaneously performed.

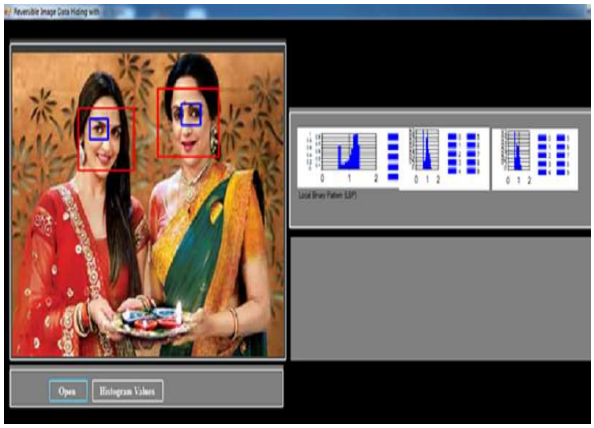

Fig. 2. Pre-processing and Histogram Calculation

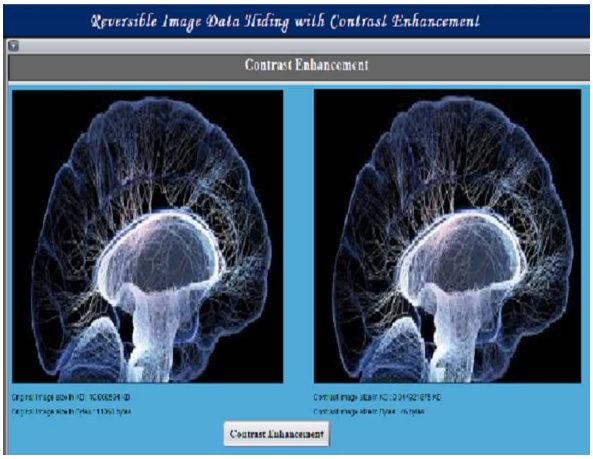

Fig. 3. Contrast Enhancement Effect

4.3. *Homomorphic Encryption*

Data is encrypted by Homomorphic encryption.In Fig.4, we show the quality of the sketch images, where the first image is original images, and the second image give the corresponding sketch images obtained.

4.4. *Embedding of Encrypted Data*

The encrypted data is embedded in the sketch image which is obtained by homomorphic en-cryption.

4.5. *Extraction and Recovery*

Ciphertext is extracted by encrypted image.Then plaintext is decrypted from en-crypted text.The original image is also recov-ered from the encrypted image.

Fig. 4. Effects of Homomorphic Encryption

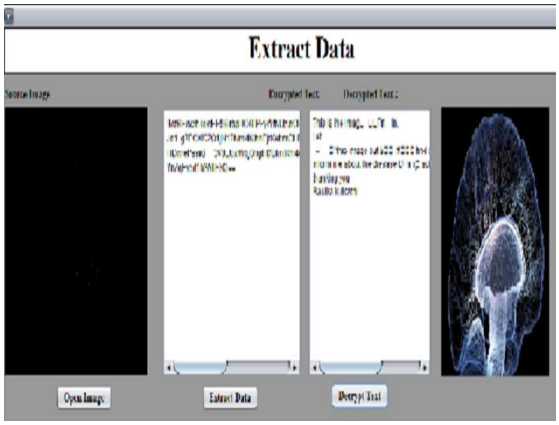

Fig. 5. Extraction and Recovery

4.6. *Robustness*

The security of the proposed image encryption scheme mainly depends on the security of the ciphertext sequence , which relies on the under-lying cryptosystem we used. If we work with the cryptosystem which has been proved to be semantically secure, e.g., the Paillier cryptosys-tem, the security of is automatically achieved.

A ciphertext-only attack (COA) is one where the assailant tries to deduce the secret key by only watching the ciphertext but It is not possible in our case because homomorphism is used for encyption so it is very difficult to deduce the secret key.

A known-plaintext attack (KPA) is one where the attacker has a amount of plaintext and the associated ciphertext but we are using the homomorphic encryption scheme in which finding out the relation between plaintext and ciphertext is very hard.

A chosen-plaintext attack (CPA) is one where the attacker picks or selects plaintext and is then given the relating ciphertext but this is also not possible in our system [16].

A chosen-ciphertext attack (CCA) is one where the attacker can have access to the de-coder, and thus can chooses ciphertext and ob-tain the relating plaintext but obtaining plain-text is impossible due to homomorphic prop-erty [16].

5. CONCLUSION

A reversible data hiding algorithm has been proposed with the property of contrast en-hancement. Fundamentally , the two peaks implies the highest two bins, in the histogram are selected for data embedding therefore his-togram equalization can be simultaneously per-formed by repeating the process. Image contrast can be enhanced by splitting a number of histogram peaks pair by pair. The original image can be exactly recovered without any additional information. Hence the proposed algorithm has performed the image contrast enhancement reversible. For improving the algorithm robustness, the Homomorphic encryption is used in proposed system. Homomorphic encryption provides the security. The proposed system is applicable to the medical images.In future,this system will be work on videos.

REFERENCES

[1] Tian, Jun. ”Reversible data embedding using a difference expansion.” IEEE Trans. Circuits Syst. Video Techn. 13, no. 8 (2003): 890-896.

[2] Ni, Zhicheng, Yun-Qing Shi, Nirwan Ansari, and Wei Su. ”Reversible data hiding.” Circuits and Systems for Video Technology, IEEE Transactions on 16, no. 3 (2006): 354-362.

[3] Thodi, Diljith M., and Jeffrey J. Rodrguez. ”Expansion em-bedding techniques for reversible watermarking.” Image Processing, IEEE Transactions on 16, no. 3 (2007): 721-730.

[4] Coltuc, Dinu, and J-M. Chassery. ”Very fast watermarking by reversible contrast mapping.” Signal Processing Letters, IEEE 14, no. 4 (2007): 255-258.

[5] Yang, Ying, Xingming Sun, Hengfu Yang, Chang-Tsun Li, and Rong Xiao. ”A contrast-sensitive reversible visible image watermarking technique.” Circuits and Systems for Video Technology, IEEE Transactions on 19, no. 5 (2009): 656-667.

[6] Sachnev, Vasiliy, Hyoung Joong Kim, Jeho Nam, Sundaram Suresh, and Yun Qing Shi. ”Reversible watermarking algo-rithm using sorting and prediction.”Circuits and Systems for Video Technology, IEEE Transactions on 19, no. 7 (2009): 989-999.

[7] Li, Xiaolong, Bin Yang, and Tieyong Zeng. ”Efficient re-versible watermarking based on adaptive prediction-error expansion and pixel selection.” Image Processing, IEEE Transactions on 20, no. 12 (2011): 3524-3533.

[8] Zhang, Xinpeng. ”Reversible data hiding in encrypted image.” Signal Processing Letters, IEEE 18, no. 4 (2011): 255-258.

[9] Fallahpour, Mehdi, D. Megias, and Mohammed Ghanbari. ”Reversible and high-capacity data hiding in medical im-ages.” IET image processing 5, no. 2 (2011): 190-197.

[10] Zhao, Zhenfei, Hao Luo, Zhe-Ming Lu, and Jeng-Shyang Pan. ”Reversible data hiding based on multilevel histogram modification and sequential recovery.”AEU-International Journal of Electronics and Communications 65, no. 10 (2011): 814-826.

[11] Zhang, Xinpeng. ”Separable reversible data hiding in encrypted image.”Information Forensics and Security, IEEE Transactions on 7, no. 2 (2012): 826-832.

[12] Wu, Hao-Tian, and Jiwu Huang. ”Reversible image wa-termarking on prediction errors by efficient histogram modification.” Signal Processing 92, no. 12

(2012): 3000-3009.

[13] Gao, Ming-Zhi, Zhi-Gang Wu, and Lei Wang. ”Comprehensive Evaluation for HE Based Contrast Enhancement Techniques.” In Advances in Intelligent Systems and Applications-Volume 2, pp. 331-338. Springer Berlin Heidelberg, 2013.

[14] Jose, Rintu, and Gincy Abraham. ”A separable reversible data hiding in encrypted image with improved perfor-mance.” In Emerging Research Areas and 2013 Interna-tional Conference on Microelectronics, Communications and Renewable Energy (AICERA/ICMiCR), 2013 Annual International Conference on, pp. 1-5. IEEE, 2013.

[15] Payal V. Parmar, Shraddha B. Padhar Survey of Various Homomorphic Encryption algorithms and Schemes Inter-national Journal of Computer Applications (0975 8887) Volume 91 No.8, April 2014

[16] Yunyu Li, Jiantao Zhou, and Yuanman Li Ciphertext-Only Attack on an Image Homomorphic Encryption Scheme with Small Ciphertext Expansion 2015 ACM. ISBN 978-1-4503-3459-4/15/10

[17] Wu, H., J. Dugelay, and Y. Shi. ”Reversible Image Data Hiding with Contrast Enhancement.” IEEE Signal Process-ing Letters, VOL. 22, NO. 1, January 2015.