THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-10-November-2019

Reversible Data Hiding With Contrast Enhancement And Encryption For Biomedical Applications

Aswathy Bhooshan, Dr Sreeni K.G , Dr Pradeep R, Dr Sajith V

Dept. of Electronics and Communication Engineering, College of Engineering, Trivandrum, India

aswathybhooshan@gmail.com

THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-10-November-2019

Abstract—Here a reversible data hiding(RDH) algorithm is proposed for biomedical applications.secret data or details is hidden inside the biomedical image for the security purpose.Data and the input biomedical image is restored without any distortion in the final stage. Instead of keeping the high PSNR value of the image, the algorithm for proposed method enhances the contrast of a host image to improve its quality of visual image. Data that has to be hidden inside an biomedical image because of security reason is restored successfully with the use of encryption and decryption.Histogram equalization is performed by data embedding in highest of two bins. This paper suggests an efficient image crypto system,which is based on simultaneous permutation and diffusion functions. That process the image pixels in a dynamic order. The proposed method employs the Chebyshev-Chebyshev map to vertically and horizontally mix the plain-image information data. Then it uses the modified Logistic map to mask the image pixels and shuffle the masked values simultaneously. To our best knowledge, it is the rst algorithm that achieves image contrast enhancement by RDH and an effective image cipher based on simultaneous permutation and diffusion operations which exhibits better performance against various attacks.

Index Terms—reversible data hiding, Contrast enhancement, histogram modication, location map, permutation and diffusion

I. INTRODUCTION

REVERSIBLE DATA HIDING (RDH) has plethora of applications and has studied in the community of signal processing and biomedical researches. Also said as reversible and lossless data hiding, RDH is used to en roo t a piece of data or information in to a host signal to generate the watermarked one, from which the original or input signal can be exactly recovered after extracting the data embedded.This technique of RDH is applicable in some sensitive and secured applications where durable change is not allowed on the input signal.In the given paper,the proposed algorithms are for biomedical images to embed secured data(e.g.[1][3])or a visible watermark which can recover the original image without any distortion from the watermarked image after the hidden data have been restored. Although the PSNR of a watermarked image produced with a prediction error based algorithm is comparatively made high,the quality of visual image can hardly be increased since more or less distortion has been introduced by the embedding process of the data.For the images acquired with poor clar-ity,improving the visual image quality is more important than keeping high PSNR value. Contrast enhancement of medical images or satellite images should show the desired details for visual verification. Although the PSNR value of the enhanced image is less, the clarity of image details of hidden data has been increased. The chaotic-based ciphers have shown excellent performance in the area of signal processing, this is because of its ability to imitate the required character of better crypto systems. These features include extreme sensitivity,noise like behavior, ergodicity in starting control parameters.Considering all these characters,lot of image ci-phers based on chaos systems have been introduced.Previous methods uses traditional permutation-diffusion structure in which two iterative stages of permutation and diffusion are used.The general permutation and diffusion architecture for image cipher is shown in Fig-3. This form is consist of two main factors,they are permutation and diffusion operations. The first one only shuffles the positions of the plain-image, with the use of 2D chaotic map such as Standard map, Cat map etc to interrupt the correlation between the neighbouring pixels. But the second operation sequentially changes the pixels values of the permuted image by a quantized chaotic key stream to distribute any small change of any pixel to almost all image pixels. Thus the whole architecture of the system is iterated to enhance the encryption effect of algorithm.

II. EMBEDDING OF DATA BY HISTOGRAM MODICATION

A. Histogram Modication technique for data embedding This algorithm used is primarily used for gray-level images but it can expand to color images easily. An 8-bit gray-level image is given , and the histogram of image can be calculated by counting the pixels with a gray-level value of the image

.Assume, it consists of different pixel values for the image.and then there are non empty bins in h1, from which the two peaks(highest of two peaks) are selected and the smaller and bigger values of peak that are considered are denoted by and Is and IR,respectively.Data embedding is performed by

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

Here i' is the new pixel value which is modified,and is the k-th message bit (0 or 1) that has to be hidden. By applying Eq.(1) to all pixel counted in totally binary values that are embedded.There is no bounding value (0 or 255) in given and in other preprocess is needed.sometimes there might be bins in the histogram that was modified. ie,the bins in between the two higher peaks are not changed while the outer most are shifted outward since each peaks can be split into two adjacent bins. The peak values Is and IR should be provided to extract the embedded data from the image. The

ISSN:0971-1260

Vol-22-Issue-10-November-2019

better method to keep them is to exclude 16 pixel from histogram computation. The least signicant bits (LSB) of that pixel value calculated are collected and included in the binary values that has to be hidden.

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

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

The peak values and need to be provided to extract the embedded data. One way to keep them is to exclude 16 pixels in from histogram computing. The extraction operations are performed in the same order as that of the embedding operations. According to Eq.(1), the following operation is perform done very pixel counted in the histogram to recover its original value.

B. Pre-Processing technology for complete recovery Overow or underow will be caused due to histogram shifting,If there is any bounding pixel value ,that is between(0 or 255), To overcome that, the pre-processing technique is used so that the image resizing can be done.Pre-processed should be done before histogram modication operations. Especially, the pixel values of 0 and 255 that causes overflow and underflow are modied to 1 and 254.. Therefore, the overflow and underflow problem can be eliminated . To remember the pixels that was pre-processed ,a location map is generated with the same size as the original image by allocating to the location of a pixel that was modified, and 0 to that of an not changed one (by including the 16 excluded pixels).Pre computation of location map can be done and that can be included into the binary values of the pixel that has to be hidden. In the generation and restoring process, data is obtained from the data generated from the watermarked images that the pixels modied in the pre-process can be recognized easily. By restoring the original values of the pixels accordingly, the original image or the input image can be completely recovered.

C. Contrast Enhancement Two peaks in each histogram is split in to two adjacent bins with the identical or similar heights because the numbers of 0s and 1s in the message bits should be equal. To improve the rate of hiding, the highest two bins in the new histogram are selected again by applying Eq. (1) to every pixel in the histogram. The similar method can be performed again by splitting each of the two peaks into two adjacent bins with the identical heights to brig off the histogram equalization effect. Data embedding and contrast enhancement are performed together. Given that the pair number of the histogram peaks to be split is ,the range of pixel values from 0 to are added by while the pixels from to 255 are subtracted by in the pre-process (noting L is a positive integer). A location map is generated by assigning 1s to the modied pixels, and 0s to the others. The location map that has computed can be embedded in input image which is also the host image. In the image retrieving process, the last split peak values of the image are extracted and the data embedded with them are retrieved with Eq. (2). After restoring the histogram with the use of Eq. (3), the data embedded with the earlier split peaks can also be extracted by processing them pair wise. At last, the location map is obtained from the extracted data to identify the pixel values modied in the pre-process.

D. Technique used in Proposed Algorithm The proposed algorithm has a procedure which is shown in Fig. 1. following steps are included in embedding procedure:

1) Pre-process: The range of (0,L-1) and (256-L,255) of pixel value are processed by not including the rst 16 pixels in the bottom row. To memorize the pixel value location map is generated.

2) Calculation of image histogram is done without counting the rst 16 pixels in the last or the bottom most row.

3) Embedding process: The two bins of the highest peaks in the histogram are split for embedding of data for the histogram modification purpose. The too peaks in the modified histogram is selected for pair splitting. Before the message bits the bit stream of the compressed location map is embedded and that will be a binary value.

4) Replacement of the LSBs of the 16 excluded pixels to form the watermarked image is done by last split paek values.

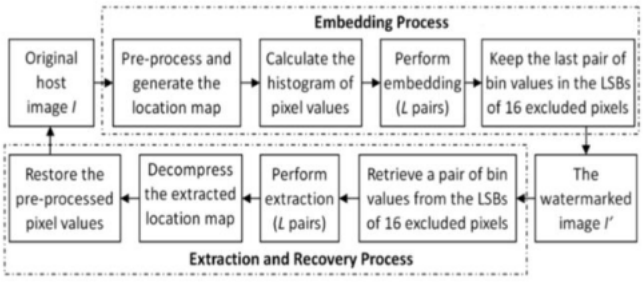

Fig. 1. RDH procedure

ISSN:0971-1260

Vol-22-Issue-10-November-2019

III. DATA ENCRYPTION AND DECRYPTION

A systematic image encryption technique that combines two basic operations permutation and diffusion together in one method is used in proposed method. Namely, both of the techniques are applied together.The mechanism that is used for diffusion is a dynamical pixel order which is suggested. The cryptosystem for image first combine image pixels in horizontal and after that in vertical directions with a key-stream is obtained in advance with the use of Chebyshev-Chebyshev chaotic map. The modified Logistic map is used to create both a dynamic pixel order and diffusion key-stream that are used to together to modify and permute the image pixels. The parameters that are used initially for the employed chaotic map, at each pixel, are dynamically taken based on the cipher-image information details, which guarantees a distinct key-stream is obtained for the distinct plain-images. So the obtained cipher can advantageous in withstanding different attacks including the most powerful chosen plain text/cipher text attack. Also, the proposed scheme takes into account the dynamic degradation problems related with chaotic systems. Simulation results and security study at test that the proposed cipher technique that is used here is more efficient and far better than any other methods and has several intense cryptographic characteristics. Along with that, after the several numerical computations and test it is also proved that the proposed cryptosystem performs several related image ciphers in terms of encryption quality and performance.

Fig. 2. Proposed method

IV. IMAGE CIPHERING STEPS

Step 1:Obtain the intermediate keys for horizontal and vertical pixel mixing measurements. 1.1 Chebyshev-Chebyshev chaotic map is iterated. 1.2 Compute the keys which is intermediate.

Step 2: Mixing of image pixels in Horizontal and vertical pixel mixing method 2.1 Mix the pixels information of the plain-image P by sequentially chaining them through XOR operation. 2.2 Apply the mixing operation in vertical direction.

V. EXPERIMENTAL RESULTS

With test done we can see that the data that was embedded were-enhanced images. The more histogram peaks were split for data

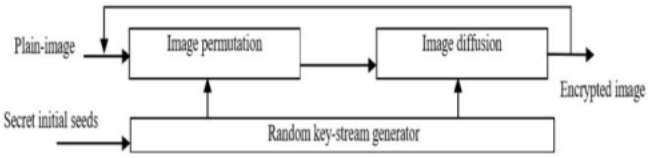

Fig. 3. Image ciphering architecture

also decreases. Even though the PSNR value of the contrast-enhanced images decrease with the data hiding rate, the quality of the visual image id preserved. Embedding capacity is also increased.

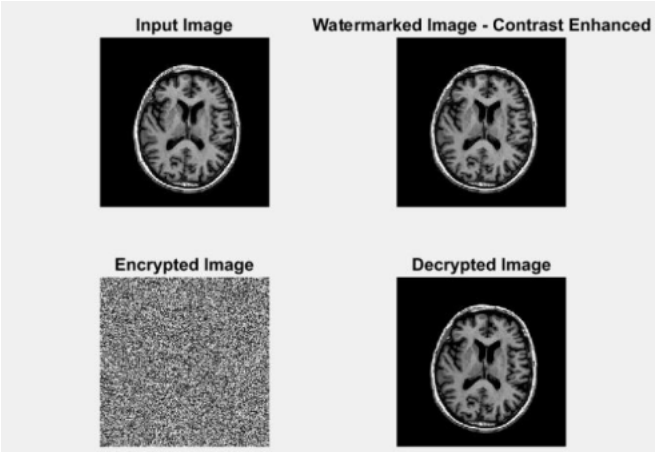

Fig. 4. Image obtained in different stages

embedding, the more contrast enhancement effect was obtained. The more data is embedding,the PSNR value

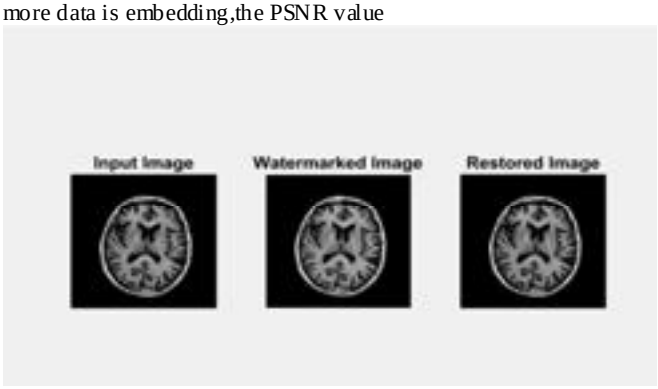

Fig. 5. Restored image comparison with input image

The results evaluated shows that the visual quality can be preserved after a considerable number of message bits have been embedded into the contrast-enhanced images,For the extraction of the original image, the location map is embeddedinto the host image, along with the message bits and other side information. So blind data extraction and complete restoration of the original image or the input image are both enabled.Better image quality is also achieved.

ISSN:0971-1260

Vol-22-Issue-10-November-2019

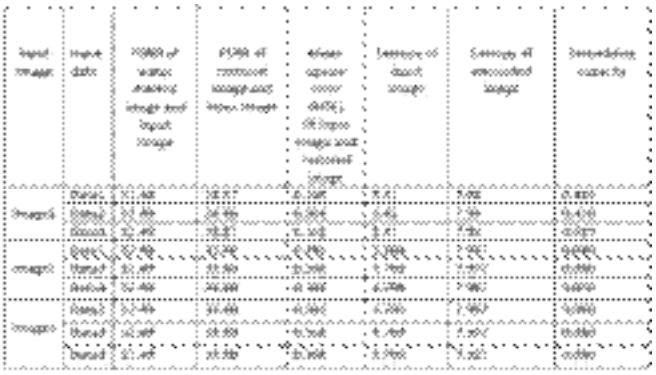

Fig. 6. Table-Output data obtained

VI. CONCLUSION

A reversible data hiding algorithm has been proposed with the property of contrast enhancement and encryption is carried out here. Basically, the two peaks (i.e. the highest two bins) in the histogram are selected for data embedding so that histogram equalization is performed simultaneously by process repetition. The results of the experiment shows that the image contrast can be enhanced by splitting a number of histogram peaks pair by pair. Visual image is obtained with better quality .This paper suggested a brilliant image cipher based on simultaneous permutation and diffusion operations together to give better result. These operations handled the pixels in a dynamic pixel order, which is chaotically produced based on image information. The proposed method uses the Chebyshev-Chebyshev chaotic map and the new Logistic chaotic map with dynamic control parameters to implement this structure. Simulation results and security study details proved that the suggested cipher has several efficient features and better performance against different types of attacks. Thus, the proposed cryptosystem is strongly appropriate for practical image security applications as well as biomedical applications.

REFERENCES

[1] J. Tian, Reversible data embedding using a dif-ference expansion, IEEE Trans. Circuits Syst. Video Techno l., vol. 13, no. 8, pp. 890896, Aug. 2003.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354362, Mar. 2006.

[3] D. M. Thodi and J. J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process., vol. 16, no. 3, pp. 721730, Mar. 2007.

[4] D. Coltuc and J.-M. Chassery, Very fast watermarking by reversible contrast mapping, IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255258, Apr. 2007.

[5] S. El Assad, and M. Farajallah, A new chaos-based image encryption system, Signal Processing: Image Communication, vol. 41, pp. 144157, 2016.

[6] B. Wang, Y. Xie, C. Zhou, S. Zhou, and X. Zheng, Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps, Optik, vol. 127, no. 7, pp. 35413545, 2016.

[7] Y.P. Li, C.H. Wang, and H. Chen, A hyper-chaos based image encryption algorithm using pixel-level permutation and bit-level permutation, Optics and Lasers in Engineering, vol. 90, pp. 238246, 2017.

[8] J. Fridrich, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcation Chaos, vol. 8, no. 6, pp. 12591284, 1998. [5] G. Chen, Y. Mao, and C. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps,