ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 4, Issue 7, DOI:10.29027/IJIRASE.v4.i7.2021.802-806, January 2021

Secured Reversible Data Hiding using Histogram Shifting Method

S. Annie Samlin[1], C. Vinoth Kumar[2] , S. Joseph Gladwin[3]
[1,2,3] Department of Electronics and Communication Engineering,
P.G. Scholar, SSN College of Engineering, India
Email: anniesamlin97@gmail.com[1], vinothkumarc@ssn.edu.in[2], josephs@ssn.edu.in[3]

***Abstract*—The Internet has become one of the significant ways of communication. Sending medical information from one place to another sometimes may cause leakage or interruption in the messages that are being sent. Thus it is necessary to protect the patient's medical information being sent through the network. Cryptography, Steganography are some of the various techniques that are being used to protect data from the outside world. Here, the patient's information is encrypted using chaotic encryption and the image is compressed by The Absolute Moment Block Truncation Coding (AMBTC) compression method. The chaotic encryption is employed in the system to improve robustness against security vulnerabilities. The compressed image is embedded into the cover image by the histogram modified embedding method. Various keys are used for encrypting and embedding the information into the image. The reverse process is done on the receiver side to retrieve the original image and the patient's information without any loss or distortion by using the same key. The Peak Signal to Noise Ratio (PSNR) of this method is obtained above 50dB.**

***Keywords*— AMBTC, Encryption, Histogram Shifting, Reversible data hiding.**

I. INTRODUCTION

Due to the rapid advancement of technology worldwide, data from various activities such as replication, leakage, interception, etc. must be secured. By using reversible data hiding techniques, the transmitted data or information can be shielded. Data hiding is a technique in which the hidden data is inserted into the original image and a stego image is created that will be the same as the original image. Reversible data hiding and Irreversible data hiding are the two major classifications of data hiding. In reversible data hiding, the compression ratio is often lower because it takes more data to restore the original image. In irreversible data hiding, the original image cannot be recovered properly even if the data is being extracted accurately. The transfer of a patient's medical information over the internet or a wired or wireless system may lead to leakage or duplication. Thus by compressing the patient's information with AMBTC and embedding by histogram modified embedding method avoids the detachment of patient information.

Difference expansion [1]-[2], prediction error expansion [3]-[4], and histogram-based shifting [5]-[7] are the various reversible data hiding techniques that are proposed under various categories. To predict the expansion of the value difference, the neighbouring pixels are used for prediction and the expansion of the prediction error allows use of the neighbourhood pixels. Expansion of prediction error uses a large prediction sense as the primary distinction between expansion of prediction error and development of difference is opposed to that of expansion of difference. The two parameters used to calculate the robustness of reversible hiding of data are distortion and payload power.

Since all the images on the internet are compressed images, the AMBTC compression method is being used to protect the data from the outside world. Delp and Mitchell proposed a method called Block Truncation Coding (BTC) [8], a lossy compression method and loses some original image data during compression. Since BTC has low computational cost, it is being used in various image compression and video compression applications. To overcome the disadvantages of BTC, Lema and Mitchell proposed a new method called AMBTC [9]-[10], which reduces the computational complexity.

Reversible data hiding [11]-[12] is an algorithm where the original image is recovered without distortion or loss even after the hidden data is extracted. Here, in order to embed the data into the image, the Zero Point (ZP) in the histogram is searched and the grayscale pixel values are modified slightly. The PSNR value is being increased to 48dB when compared to that of the previous methods. The computational complexity is also reduced since it involves only scanning, adding operations, and finding maximum or minimum points and does not involve in complex operations like Discrete Fourier Transform (DFT) or Fast Fourier Transform (FFT). The execution time is low since it requires only 100ms for embedding 5 to 80 KB of data into a 512x512x8 grayscale image.

Many Reversible Data Hiding techniques that are proposed. Histogram shifting is one of the most commonly used reversible data hiding schemes. By using the minimum points in a histogram[13], Zhicheng Ni et al suggested an RDH scheme. A pair of Peak Point (PP) and ZP will be obtained to embed the data. The residual histogram is a technique of embedding a histogram that is used to increase the capability of embedding. Residual histogram shifting is performed in compressed images in order to decrease the storage space.

Chaos-based encryption is one of the encryption methods that is used in recent days. Chaotic encryption [14]-[15] is a multidisciplinary system that creates a logistic function and then does the circular shifting operation to obtain the key. To avoid attacks, a random sequence of keys are generated. Only the authorized receivers can extract the data and restore the original information. This encryption method can be used in real-time since it has a simple algorithm and low computational complexity.

This study presents the histogram embedding method which deals with the concept of shifting the PP and the ZP with high payload capacity and low storage. The AMBTC compression method is used to compress the patient information into the cover image to avoid leakage of information. By integrating with the chaos-based encryption, attacks can be avoided in the system. The original image can be decrypted, decoded and restored only by the users with the data hiding key. The proposed framework and the results obtained are discussed in the further sections.

II. Proposed System

The secret data is being embedded into the original image by using a reversible data hiding embedding algorithm along with the secret key at the embedding stage. The process of reversible data hiding is shown in Figure 1. During the chaotic encryption process, the patient information is encrypted and then compressed using the AMBTC compression method. The patient information is embedded into the cover image, encrypted and the stego image is obtained. Data extraction and recovery are used to restore the original image and the patient information.The block diagram of the embedding process is shown in Figure 2 from which the stego image is obtained.

A. *Chaotic encryption*

The security of the image along with the data embedded is enhanced by using the chaotic encryption method. The patient information that is to be encrypted is used as an input. The logistic map function is used to generate random sequences using two parameters r = 3.62 and x_1 = 0.7 using the Eqns. (1).

$$X_{n+1} = r X_n (1- X_n) \qquad (1)$$

The key K1 is generated by using the logistic map function. Key K2 is obtained by linearly circular shifting the random sequence that is generated by the logistic map function. Keys K1 and K2 are XORed to get the encrypted text. The encrypted image is obtained by XORing the key of the encrypted image with the patient information.

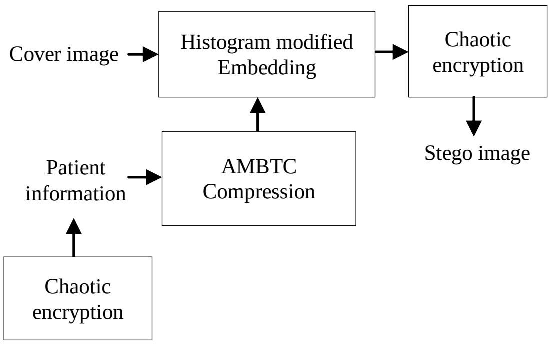


Fig. 1 Process of reversible data hiding

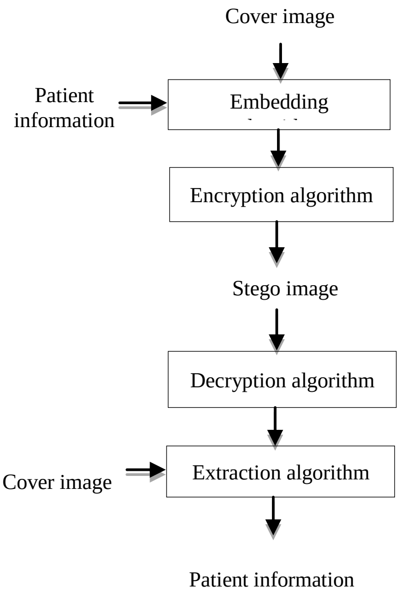


Fig. 2Block diagram of the embedding process

B. *AMBTC*

Delp and Mitchell introduced a technique for image compression called Block Truncation Coding (BTC). The BTC algorithm is a simple, block-based and spatial domain. BTC is a lossy compression technique that is being considered as highly efficient compression techniques for decades. The AMBTC works in the same way as that of BTC except only two mean values are calculated instead of mean and standard deviation. In 8 to 8 non-overlapping blocks, the patient information collected after encryption is sub-divided. The average values of all the blocks are being evaluated. In order to restore the original image, each block is stored as one bit map and two quantization levels, called high mean value and low mean value. The sample mean and absolute moment is calculated using the following Eqns. (2) and (3).

$$\eta = 1/m \sum_{i=1}^{m} x_i \qquad (2)$$

$$\sigma = \sqrt{\{1/m \sum_{i=1}^{m} x_i^2 - \eta^2 \}} \qquad (3)$$

where $x_i$is the i^{th} pixel value, m It denotes the number of pixels whose values are below µ.The AMBTC reduces the complexity of computation and retains each block's central moment and high image efficiency. The compression bitmap is defined as follows: if at that position the pixel value is less than µ, it is set to 0, otherwise it is set to 1. The bit value 0 is then restored as a low mean value when approximating the grayscale picture and the bit value 1 is restored as a high mean value..

C. *Histogram modified embedding*

In the histogram modified embedding method, the PP is obtained from the residual histogram and the position of the pixels to its left and right are being shifted by one, as shown in Figure 3. The patient information is embedded in the block, which has the highest payload. A separate key is given for each block to extract the data at the receiver side.

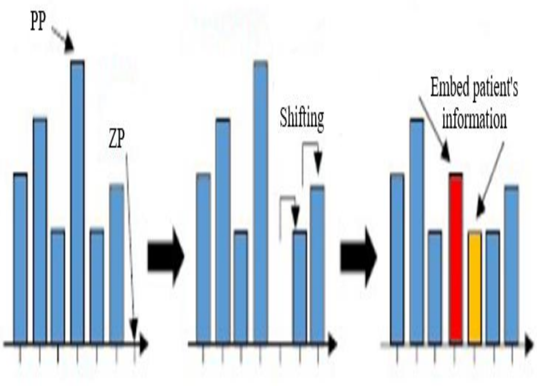


Fig. 3 Histogram embedding method

During the data embedding stage, the entire image is scanned pixel by pixel in a specific order. Figure 4 demonstrates the method of histogram-modified embedding. To insert the hidden data, the PP is first taken. If the corresponding hidden bit is 1, the pixel value is changed to fill the empty bin near PP. But, if the bit you want to embed is 0, the value of the pixel does not change. To get a perfect restoration of the cover at the receiving end, the position of PP and ZP is also given to the receiver hand, along with the patient information.

This technique's capability will be equal to the number of pixels in PP. If the payload is greater than the number of pixels in PP, then the remaining data is embedded by the second pair of PP and ZP. The stego image is acquired after embedding the data with the data embedded within it.

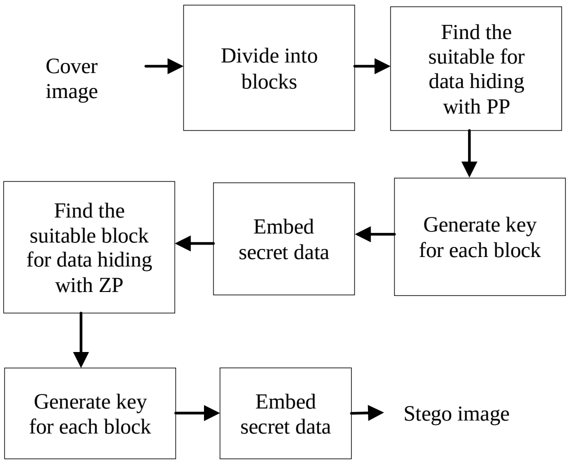

Cover image
Divide into blocks
Find the suitable for data hiding with PP
Generate key for each block
Embed secret data
Find the suitable block for data hiding with ZP
Generate key for each block
Embed secret data
Stego image

Fig. 4 Procedure of histogram modified embedding

D. Data extraction and image recovery

The extraction of the AMBTC compressed patient information and the recovery of the original image is explained in this section. The process of recovery and extraction is shown in Figure 5. The stego image obtained is being decrypted using a chaotic decryption method. The embedded patient information is extracted by using the histogram modified de-embedding process where the original image is recovered without any loss. If the correct key is used by the receiver that is sent from the transmitter side, then the image will be recovered correctly. Then by using the AMBTC decompression method, the patient information is extracted properly.

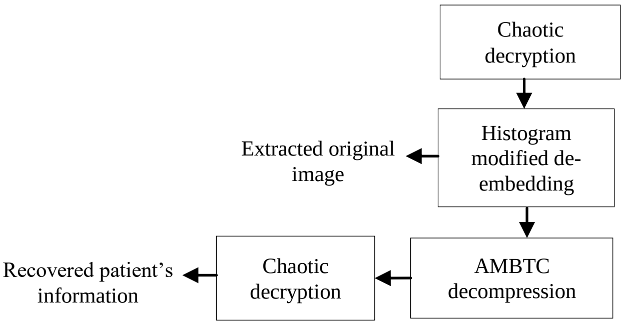
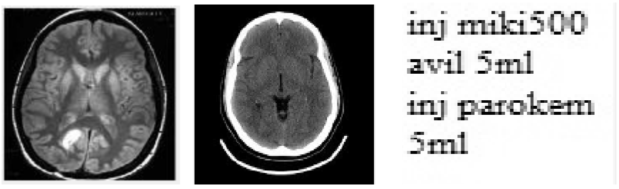


Fig. 5 Block diagram of extraction process

III. Results And Discussion

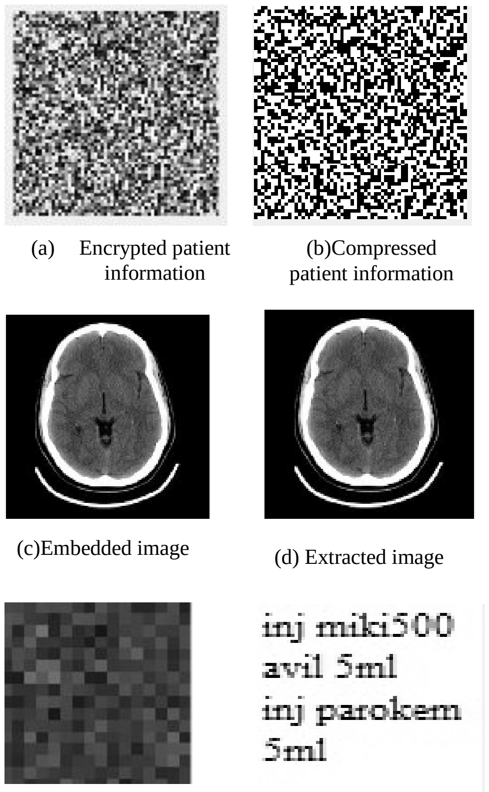
The performance analysis of the reversible data hiding technique and the experimental results are discussed in this section. The performance metrics used for the reversible data hiding technique are PSNR, Embedding capacity, MSE, and SSIM. PSNR is the most common metric used to appraise the quality of the stego image. The PSNR represents the measure of peak error. The lower the value of the MSE, the lower is the error. The patient information is encrypted by the chaotic encryption method and compressed using the AMBTC compression method and it is embedded using the histogram modified embedding process. The original image and the data embedded are extracted from the stego image using the histogram modified de-embedding process. The encrypted patient information, compressed patient information, stego image are shown below in Figure 6.


inj miki500
avil 5ml
inj parokem
5ml

(a) Brain (b) CT scan :c) Patient information

Fig. 6 Cover images and patient information.

The encrypted patient information using the chaotic encryption method is shown in Figure 7(a), where it is compressed using the AMBTC method with high and low mean values in Figure 7(b). In Figure 7(c) the stego image is obtained along with the information embedded into the cover image by using the histogram embedding method. At the receiver side, the cover image is extracted separately in Figure 7(d). Figure 7(e) shows the decompressed patient information by using the AMBTC decompression method where the 0 and 1 are replaced by the high mean and low mean values. By using the chaotic decryption process through logistic de-mapping, the patient information decrypted is shown in Figure 7(f).



(a) Encrypted patient information

(b)Compressed patient information

(c)Embedded image

(d) Extracted image

(e) Decompressed patient information

(f) Decrypted patient information

Fig. 7 Images obtained using histogram modified embedding

The cumulative square error between the compressed image and the original image is given by MSE. The lower the square error in the shot, the lower the picture's quality would be. The most common metric used to measure the efficiency of the stego image is PSNR. The PSNR reflects the peak error metric. The lower the value of the MSE the lower is the error. SSIM is a constant metric that determines the quality of image degradation caused by various processes like data compression or due to losses in compression. It signifies the similarity between the original image and the recovered image. In the below Table 1 the readings that were obtained for the two test images are tabulated. The plots that are obtained for embedding capacity vs MSE, PSNR, and SSIM for the CT scan image is shown in Figures 8, 9 and 10.

Table 1Embedding capacity vs MSE, PSNR, and SSIM

Embedding capacity					
	Imag es	64 × 64	128 × 128	256 × 256	512 × 512
MS E	Brain	2340	11340	35930	35940
	CT scan	4130	19340	2530	22540
PS NR	Brain	64.4 807	57.583 1	52.576 6	52.274 8
	CT scan	61.9 679	55.265 3	54.603 0	54.601 0
SSI M	Brain	0.99 97	0.9985	0.9960	0.9960
	CT scan	0.99 96	0.9981	0.9976	0.9976

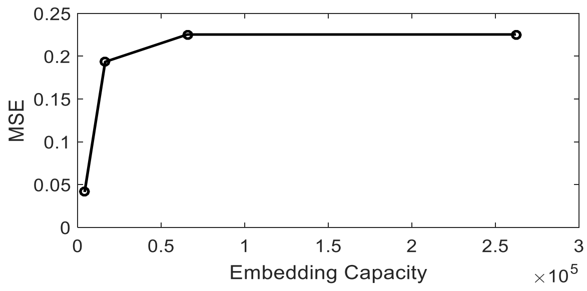


Fig. 8 Embedding capacity vs MSE

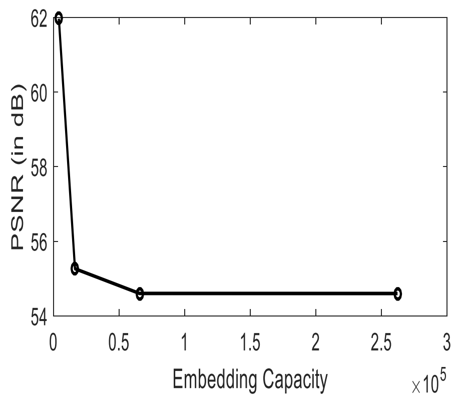


Fig. 9 Embedding capacity vs PSNR

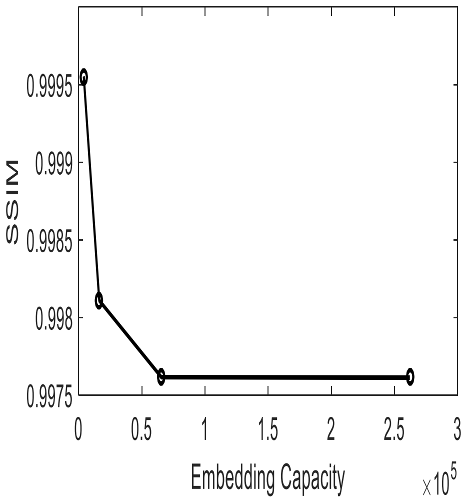


Fig. 10 Embedding capacity vs SSIM

IV. CONCLUSION

This paper describes a method for hiding the patient information within the medical image by using the reversible data hiding technique. The patient information is compressed to reduce the computational complexity by using the AMBTC compression method. Histogram modified embedding is used for embedding and retrieving the patient information properly. To secure the robustness of the system, chaotic encryption is used. The original medical image and patient information are recovered without any loss or distortion. From the simulation results, the PSNR value is found to be above 50dB.

REFERENCES

[1] Alattar, AM (2004), "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 1147-1156.

[2] Tian, J (2003), "Reversible Data Embedding Using a Difference Expansion," IEEE Transactions on Circuits and Systems For Video Technology, vol. 13, no. 8, pp. 890-896.

[3] Thodi, DM & Rodriguez, JJ (2004), "Prediction-Error based Reversible Watermarking," Proceedings of IEEE International Conference on Information Processing, vol. 3, pp. 1549-1552.

[4] Chen. H, Ni .J, Hong. W and Chen. T (2017), "High-Fidelity Reversible Data Hiding Using Directionally Enclosed Prediction," in IEEE Signal Processing Letters, vol. 24, no. 5, pp. 574-578.

[5] Che-Wei Lee & Wen-Hsiang Tsai (2011), "A Lossless Large-Volume Data Hiding Method Based On Histogram Shifting Using an Optimal Hierarchical Block Division Scheme," Journal of Information Science and Engineering, vol. 27, pp. 1265-1282.

[6] Yamato. K, Shinoda. K, Hasegawa. M and Kato. S (2014), "Reversible data hiding based on two-dimensional histogram and generalized histogram shifting," IEEE International Conference on Image Processing (ICIP), Paris, pp. 4216-4220.

[7] Ying. Q, Qian. Z, Zhang. X and Ye. D (2019), "Reversible Data Hiding With Image Enhancement Using Histogram Shifting," in IEEE Access, vol. 7, pp. 46506-46521.

[8] E. Delp and O. Mitchell (1979), "Image compression using block truncation coding," IEEE Trans. Commun., vol. 27, no. 9, pp. 1335_1342.

[9] M. Lema and O. Mitchell (1984), "Absolute moment block truncation coding and its application to color images," IEEE Trans. Commun., vol. 32, no. 10, pp. 1148_1157.

[10] Zhaoxia Yin, Xuejing Niu, Xinpeng Zhang, Jin (2018), "Reversible data hiding in encrypted AMBTC images," Multimedia Tools and Applications, Volume 77, Number 14, Page 18067.

[11] Zhicheng Ni, Yun-Qing Shi, N. Ansari and Wei Su (2006), "Reversible data hiding," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362.

[12] Zhang. W, Wang. H, Hou. D and Yu. D (2016), "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation," in IEEE Transactions on Multimedia, vol. 18, no. 8, pp. 1469-1479.

[13] J.Wang, J. Ni, X. Zhang, and Y.-Q. Shi (2017), "Rate and distortion optimization for reversible data hiding using multiple histogram shifting," IEEE Trans.Cybern., vol. 47, no. 2, pp. 315_326.

[14] Fuyan Sun, Shutang Liu, Zhongqin Li & Zongwang Lu (2008), "A novel image encryption scheme based on spatial chaos map," Chaos, Solitons & Fractals, vol. 38, no. 3, pp. 631-640.

[15] Wang. H, Lin. H, Gao. X, Cheng. W and Chen.Y (2019), "Reversible AMBTC-Based Data Hiding With Security Improvement by Chaotic Encryption," in IEEE Access, vol. 7, pp. 38337-38347.