HIDING THE MEDICAL IMAGES BY REVERSIBLE DATA HIDING

V.V. Vinoth
Research Scholar
Department of ECE
Bharath University, Chennai
India
E-mail:vinothvv.velaian@gmail.com

Dr. B. Karthik
Associate Professor
Department of ECE
Bharath University, Chennai,
India
E-mail: karthik.ece@bharathuniv.ac.in

***Abstract*- A data hiding is a technique that is used for embedding the important information into images. The degradation of the original image like medical imagery and military imagery are not allowed in reversible data hiding. The secret data is attached in the compression domain and the receiver needs to store the image in a compression mode to save storage space. An encoding data will be compressed and encrypted by the secrete key. A decode message presents the secret data that can be seen by the encrypted key. This paper proposed to hide the medical images. The experimental result shows that proposed system can provide good performance to secure important data.**

Index Terms- Medical images, Secure data, RDH

I.INTRODUCTION

The main purpose of data hiding is to extend the communication security by embedding secret messages into a hidden carrier and then transmitting it to receiver side. The embedding process will normally introduce permanent distortion and rebuild from the marked image. The uncompressed image using an encryption key to produce an encrypted image and then a data hider embeds extra data into the encrypted image using a data-hiding key. To apply reversible data hiding to encrypted images to take off the embedded data before the image decryption .The information is embedded the data that it is perceptually and analytically unpredictable .Data embedding also support an embedding valuable control and information. Reversible data embedding, which is frequently referred as lossless data embedding, is a technique that embedding the data into an image in a reversible manner. The original uncompressed image using an encryption key to produce an encrypted image and then a data hider embeds extra data into the encrypted image. To decrease the transmission time the data compression is essential. The encrypted image can be compressed by using various techniques. In Lossy compression of an encrypted image flexible compression ratio is done. The data exchange involves transmission of several types of data format like medical images, texts, and graphs. Data hiding techniques can also be used for authentication. As a persuasive means for security protection, encryption converts the ordinary signal into irregular data, so that the traditional signal processing normally takes place before encoding or after decoding.

II.REVERSIBLE DATA HIDING

A reversible data hiding is a type of process covertly embedded in a noise-tolerant signal such as audio or image data. It is used to recognize ownership of the copyright of particular signal. It is the process of hiding digital information in a carrier signal. The hidden information does not need to contain a relation to the carrier signal. It can be used to verify the authenticity or purity of the carrier signal or to exhibit the identity of its owners. It is used for tracing copyright infringements and for banknote authentication.

A data is embedded into a digital signal at each point of distribution. If a work is found later, then the data can be fetch from the copy and the source of the distribution is known. Data hiding is based on the concept of separation of the design decisions in a computer program, if the design decision is switched, which are used to protect the other parts of the program from expanded modification. The protection giving a stable connection which protects the remaining program from the implementation. Compression schemes can

4. highest spatial details. In this case, due to spatial masking of the human visual system, the subjective quality of the watermarked image will be at its best.

5. Narrower histogram: Some image tiles have much narrower histograms than that of the whole image. This is specifically true for medical images that lead to the flowing useful properties for data hiding:

a) In the broader histogram of the whole image the minimum frequency may not be zero. For reversible data hiding, their positions need to be determined and given as side information, which greatly reduce the data hiding capacity. On the other hand, in the narrower histograms of the image tiles, the minimum frequencies are more likely to be zero.

b) Narrower histograms presents the opportunities of selecting the most appropriate pairs of peaks-zeros that will improve the quality of the marked images.

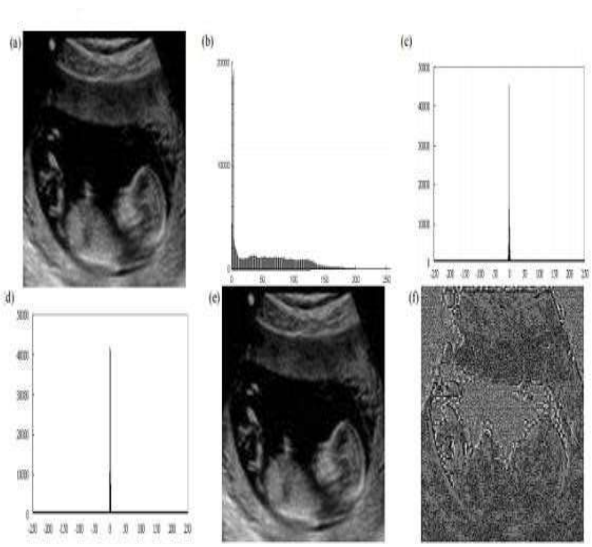

Fig 3: a) Medical Image, b) Original Image Histogram h , c) Histogram h1, d) Histogramh2, e) Stego Image, f) The difference image.

V.EXPERIMENTAL RESULT

The experimentation has been carried out using MATLAB R2014a platform for different images. We have used medical and general test images for testing our algorithm. It is assumed that size of general and medical test images is such that it is divisible by (4 × 4), i.e. it leads to integral number of 4 × 4 blocks. The medical images used for evaluating the performance of the presented scheme are shown in Fig. 4. The digital watermark used for authentication is of the size 64 × 64. The scheme has been tested for a total payload of 196,608 bits or 0.75 bits per pixel (bpp). The image quality has been established by carrying out objectivequality analysis in terms of Peak Signal to Noise Ratio (PSNR) and Structural Similarity Measure Index (SSIM) between original image and 'watermarked & attacked' image. The content authentication of the proposed scheme has been evaluated by calculating Bit Error Rate (BER%) and Normalized Cross-Correlation (NCC) between embedded 'watermark and data' and extracted 'watermark and data' for various attacks. Eqs. (1), (2), (3), (4), (5), (6), (7), (8), (9) have been used for computation of various objective quality metrics.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - x'_{ij})^2 \qquad (1)$$

$$PSNR = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{(255)^2}{MSE}\,d \qquad (2)$$

In the above formulae; M, N are the dimensions of the original image and the watermarked image; x (i, j) is the (i, j) th pixel value of original image and (x′i, j) is the (i, j) th pixel intensity value of watermarked image.

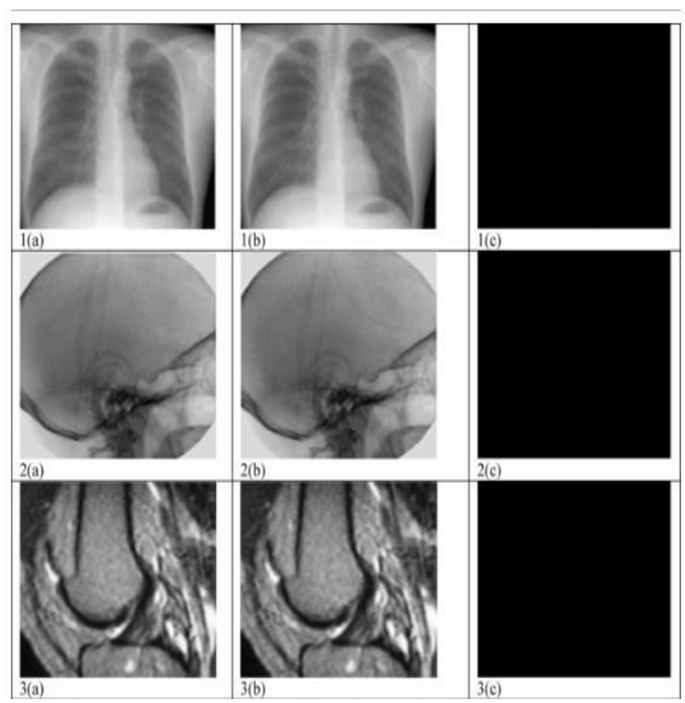

Fig 4: (1a–3a) Original images, (1b–3b) watermarked images for a payload of 0.75bpp, (1c–3c) difference of original and recovered images

The Structural Similarity Index (SSIM) is based on the calculations of three terms, namelythe luminance, contrast and structure. The overall index is a given by

$$SSIM(x,y) = [l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} \quad (3)$$

Where,

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x \sigma_y + C_3} \quad (4)$$

$$l(x,y) = \frac{2\mu_x \mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (5)$$

$$c(x,y) = \frac{2\sigma_x \sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (6)$$

where μx, μy, σx, σy, and σxy are the local means, standard deviations, and cross-covariance for images x, y. For default exponents and default selections of C3 the expression is given by:

$$SSIM(x.y) = \frac{(2\mu_x\mu_y + C1)(2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C2)} \quad (7)$$

$$BER = \frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N} W_m(i,j) + W_{me}(i,j)\right] \times 100 \quad (8)$$

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W_m(i,j) \times W_{me}(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} W_m(i,j)^2} \quad (9)$$

In above equations; M, N are the dimensions of the original logo and extracted logo; wm (i, j) is the (i, j)th pixel of original watermark and wme (i, j) is the (i, j)th pixel of the extracted logo.

VI.CONCLUSION

In this paper, we proposed to hide the medical images for transmitting the secured message. The experimental result shows that the secret data can be encoded and decoded. In future work, we will pay our attention to secret file transmitting to one place to another place.

REFERENCES

[1] Medical Image Protection by Using Cryptography DataHiding and Steganography, Vinay Pandey, Angad Singh,Manish Srivastava, ISSN 2250-2459,Volume 2,Issue1,January 2012.0

[2] Multimedia Data Embedding and Watermarking Technologies, Mitchell D. Swanson, MEI KOBA YASHI,AHMED H.TEWFIK,PROCEEDING OF THE IEEE,VOL.86,NO.6,JUNE 1998.

[3] STEGANALYSIS OF HISTOGRAM MODIFICATION REVERSIBLE DATA HIDING SCHEME BY HISTOGRAM FEATURE CODING, Der-Chyuan Lou, Chen-Hao Hu and Chung-Cheng Chiu, ICIC International©2011 ISSN 1349-4198.

[4] Histogram Modification Based Reversible Data Hiding Algorithm.K. Kishore Kumar.

[5] Secure Medical Image Transmission Using Combined Approach of Data Hiding ,Encryption and Steganography, VinayPandey, Manish Shrivastava,Volume 2,Issue 12,December 2012,ISSN:2277 128X

[6] Wakatani, A.: "Digital watermarking for ROI medical images by using compressed signature image". Hawaii International Conference on System Sciences, 2002, pp.2043-2048.

[7] Coatrieux, G., Lecornu, L., Sankur, B., and Roux Ch.: 'A Review of Image Watermarking Applications in Healthcare'. In Conference of the IEEE-EMBS, pp. 4691-4694, 2006.

[8] Ni, Z., Shi, Y. Q., Ansari, N., and Su, W.: 'Reversible data hiding'. IEEE Trans. on Circuits and Systems for Video technology, vol. 16, no. 3, pp.354-362, 2006.

[9] Macq, B., Dewey F.: "Trusted Headers for Medical Images". DFG VIII-DII Watermarking Workshop, Germany, 1999.