ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

Image Steganography Model for Medical Images Using GLM

Kamaldeep Joshi[1], Sachin Allwadhi[2], Rajkumar Yadav[3]

Department of Computer Science and Engineering, U.I.E.T, M. D. University, Rohtak, Haryana, India

Abstract: In this paper, a steganographic model in medical system is proposed using gray level modification method of image steganography. In gray level modification method the data is embedded on the pixel based on its gray value. For making a pixel suitable for adding information bit, +1 or -1 is performed on it. So, the maximum change in the image pixel is one which is admissible. Different medical images are taken for experimental result. Image is passed from one doctor to another after embedding their respective prescription in it. The experiment is performed on the seven medical images and the result is obtained.

Keywords: GLM; PSNR; MSE; MAXERR; MEDICAL IMAGING.

I. INTRODUCTION AND LITERATURE REVIEW

In modern era of communication security of message is a major concern. Achieving security leads anyone in two domains either steganography or cryptography. The prior technique is related to hiding of data while latter one uses scrambling of data [1]. Steganography uses some cover media like images to hide information (I) called Host image (H) and resultant image called Stego-image (S) i.e S= H+I. Present techniques in steganography are spatial domain and Transform domain wherein first one works over gray levels directly whereas other one transform host image from spatial domain to transform domain and information is concealed by changing image- coefficient. Popularly known technique in spatial domain such as PIT (pixel indicator technique) [2, 3], edges based embedding techniques [4, 5] while popularly known techniques in transform domain techniques such as discrete cosine transform technique [6, 7] and discrete wavelet transform technique [8]. Application domain of image steganography like medical imaging, watermarking, innocipher, GSI and so on ;medical imaging is related to hiding information about patients in medical images such as CT scans, MRIs, Ultrasounds, X-Rays or in other modalities while watermarking for copyright reservation. Based on GLM (Gray level modification) Al-Taani and AL-Issa [9] proposed a technique in which a host image is spilt into areas having same sizes and information is concealed in block's edges based on last four bits of pixel. W.Puech [10] proposed an algorithm that can be applied to images, videos and 3D objects for data hiding watermarking, encryption and compression. Al-Dmour and Al-Ani [11] proposed a technique that used Otsu's method in which host image is divided into two blocks namely ROI (Region of Interest) and RONI (Region of Non Interest). Based on Binary Pixel Intensity (BPI) ROI pixels are encased in rectangular shape and for enhancing security high frequency sub bands are used in which Electronic Patient Record (EPR) is embedded. Jain and lenka [12] provide an efficient method in image steganography in biomedical field. In this queue data structure is used for communication and message is first encrypted using Rabin Cryptosystem and results in many blocks and sub-blocks which are distributed equally. In this method, the receiver has four different values for plain text corresponding to one cipher text so that only authorized receiver can recognize the correct medical data. The diagonal queues are used for storing the different images of brain disease. J. Liu et al. [13] proposed a method in which confidentiality is maintained by steganography approach in medical images. In this, a host image is transformed into 1-D pixels sequence using Hilbert filling curve and further divided into non-overlapping groups of 3 pixels in each. Now embedding of data is based on APPM (adaptive pixel pair match) method. In which pixel value differences (PVD) of 3 pixels is taken out and data is embedded in those pixel ternaries causing minimal distortion and results show better privacy protection than previous steganography methods. Rao and kumari [14] investigated; Medical image watermarking has been widely known for increasing data security, authenticity and content justification in e-health education where medical images are used over network. Figure 1 shows the block diagram of the proposed model.

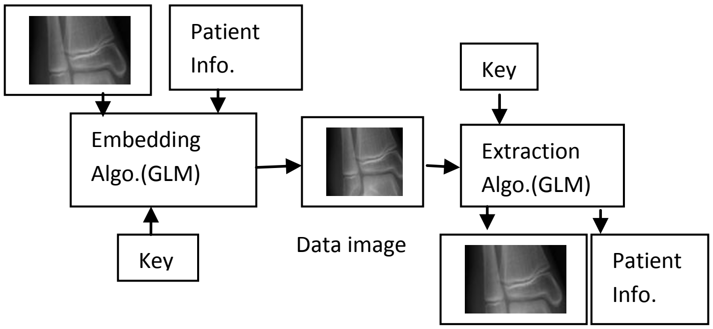


Figure 1; Block diagram of the proposed model

II. PROPOSED TECHNIQUE

Procedure starts from very first pixel (m_{oo}) of cover image (M) i.e $M = \{m_{xy\,|}\ 0<=x<R, 0<=y<C\}$ where m_{xy} represent a pixel of cover –image. Different pieces of information are added in Host image 'M' as prescriptions using Gray Level Modification Technique (GLM) and each piece of information (D) can be represented as $D = \{d_Z \mid 0<=z< l , d_z\ \varepsilon\ \{0,1\}\}$. It will be helpful to understand GLM, before going in detail of procedure. In GLM technique, adjustment are made on pixels if selected information bit is not matching with gray value of that pixel either incrementing or decrementing pixel value by 1 otherwise no changes are made as shown in following figures 2 and 3.

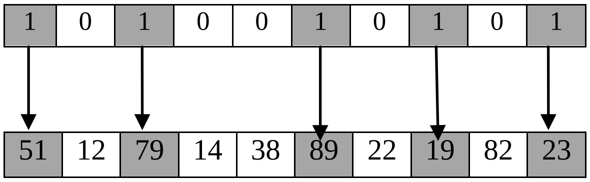


Figure 2 Embedding Gray level values

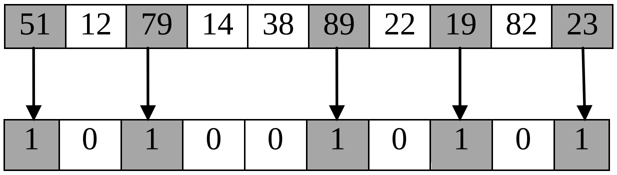


Figure 3 Retrieval data in GLM

From the very outset, insertion algorithm checks if length (L) of prescribed information i.e L < R*C where R is number of rows and C is number of column of cover media. If yes, then procedure continuous to embed information bits using GLM technique in cover media such that $n_{xy} = m_{xy}$+dz and f(x, y) = f(x,y) + 1 here pixel location can be represented by f(x,y), where x and y shows corresponding row number and column number of particular pixel in host image. On exhausting length 'L' prescription, if there exist anymore prescription of length (L_i) then procedure validates $L_{i\,<}$ R*C- L. If yes, then insertion procedure is continued again just after next pixel location where last insertion is ended up. It continues until numbers of pixels in cover-media or doctor's prescriptions are over. At the end of this procedure we get resultant stego image (N) such that $N = \{n_{xy} \mid n_{xy\,=}\ m_{xy\,+}\ d_{z,}\ n_{xy}\ \varepsilon\ \{0,1\}\ \}$ as shown in following flow chart.

PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) are taken for the performance measurement of the gray level modification method. Both are inversely proportional to each other. The value of PSNR increases when two images are close to each other whereas the value of MSE decreases when the two images are similar to each other. MAXERR gives the maximum difference between two images.

The PSNR is evaluated in decibels and is inversely proportional the MSE. It is specified by the equation:

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{\mathrm{I}^2}{\mathrm{MSE}}\right] \qquad (1)$$

Where

$$\mathrm{MSE} = \frac{1}{[\mathrm{R}\times\mathrm{C}]^2}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathrm{H}_{ij}-\mathrm{S}_{ij})^2 \qquad (2)$$

Where I denotes the dynamic range of pixel values, or the maximum value that a pixel can have for 8 bit image: I=255. R and C are the dimensions of the cover and the image having information. H_{ij} and S_{ij} are the intensity of pixels in cover and the image embedding information.

Figure 4 and 5 show the flowchart of the proposed model and histograms of the original and image concealing information respectively. Figure 5 shows the histograms of the images shown in figure 6. The histogram in figure 5 indicates that the change in original and Stego image is very low i.e. high imperceptibility. Figure 6 shows the original and the embedded information images having prescriptions from different doctors' .Table I, II and III showing the MSE, PSNR and MAXERR of cover and Stego images using the GLM method.

Table I PSNR, MSE and MAXERR of Stego image 1 concealing data size 1Kb

Images name	***PSNR***	***MSE***	***MAXERR***
Image 1	69.16	0.007	1
Image 2	68.52	0.009	1
Image 3	68.85	0.008	1
Image 4	67.50	0.011	1
Image 5	68.57	0.009	1
Image 6	69.34	0.007	1
Image 7	68.13	0.011	1

Table II PSNR, MSE and MAXERR of Stego image 2 concealing data size 2Kb

Images name	***PSNR***	***MSE***	***MAXERR***
Image 1	66.11	0.013	1
Image 2	67.00	0.013	1
Image 3	66.85	0.013	1
Image 4	65.62	0.017	1
Image 5	66.77	0.013	1
Image 6	66.08	0.016	1
Image 7	65.07	0.020	1

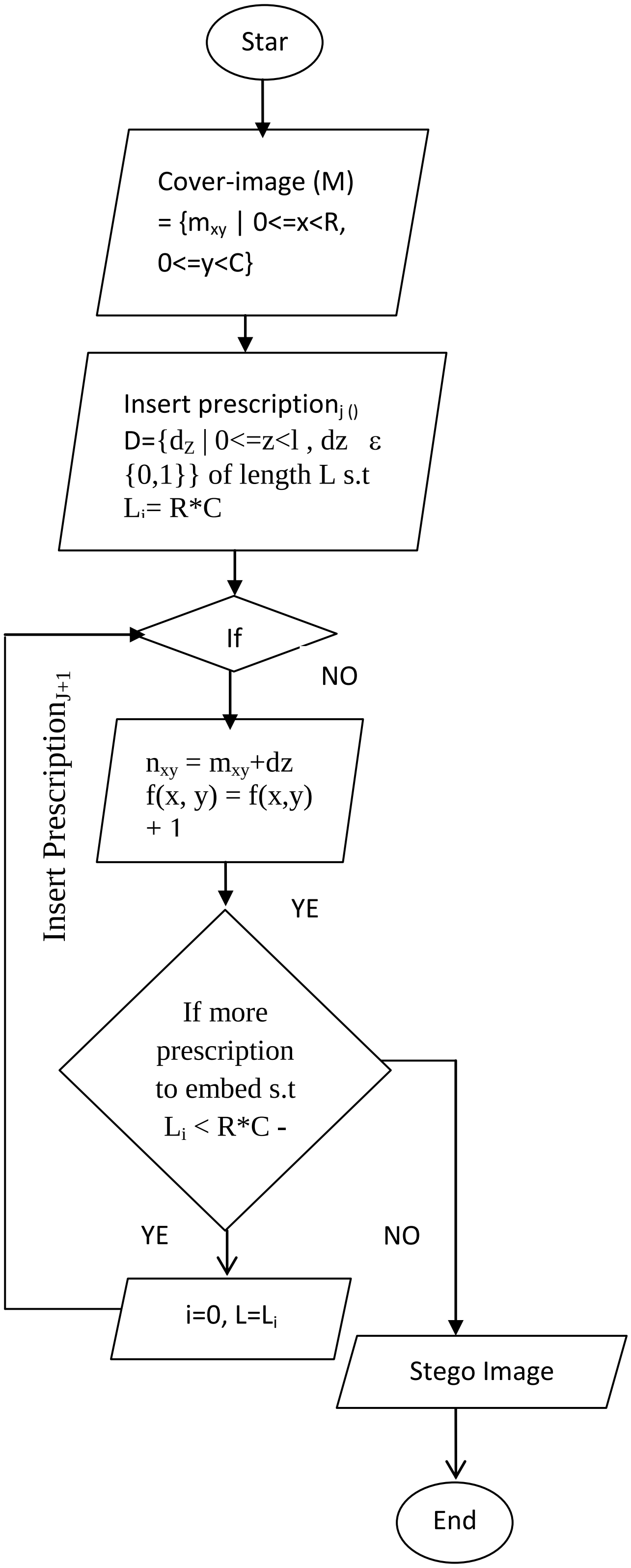


Figure 4; Flow chart of the proposed method

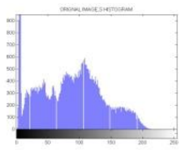
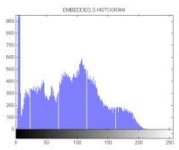
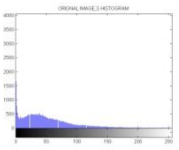
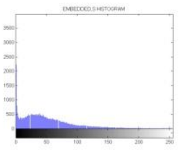
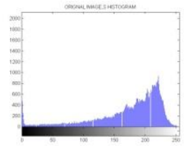
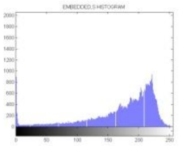
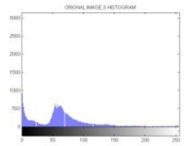
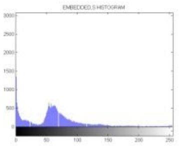
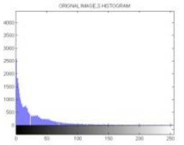
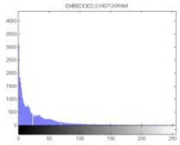
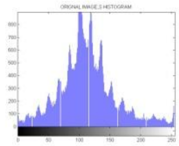
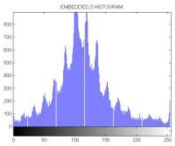
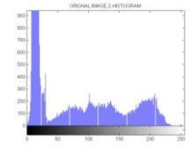
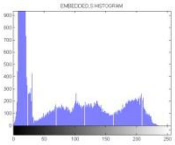
Image name	Original Histogram	Stego-image Histogram
1		
2		
3		
4		
5		
6		
7		

Figure 5; Histograms of Original and Stego images

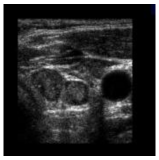
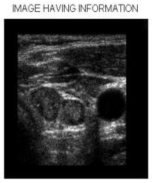
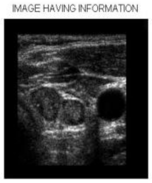
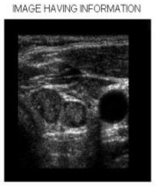
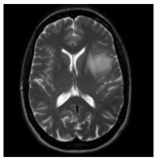
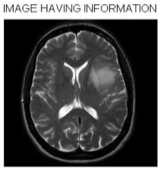
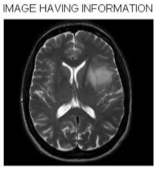
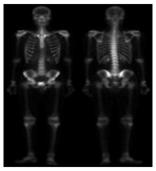
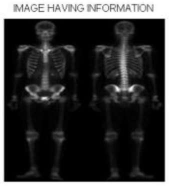
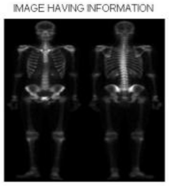
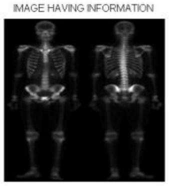
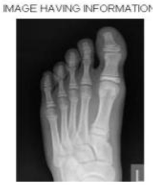
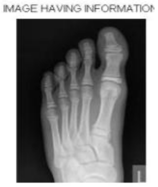
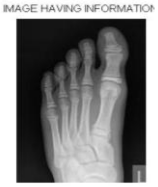
Name/Size	Host images	Doctor 1 prescription of data size 1Kb	Doctor 2 prescription of data size 2Kb	Doctor 3 prescription of data size 4Kb
		Stego image 1	Stego image 2	Stego image 3
1 (256*256)				
2 (256*256)				
3 (256*256)				
4 (225*224)				
5 (256*256)				
6 (256*256)				
7 (269*187)				

Figure 6; shows the (1) Different host images in first column (2) Doctor 1 prescription of data size 1Kb in second column (3) Doctor 2 prescription of data size 2Kb in third column (4) Doctor 3 prescription of data size 4Kb in fourth column.

Table III PSNR, MSE and MAXERR of Stego image 3 concealing data size 4Kb

Images name	***PSNR***	***MSE***	***MAXERR***
Image 1	63.04	0.032	1
Image 2	63.98	0.026	1
Image 3	63.78	0.027	1
Image 4	63.59	0.035	1
Image 5	63.80	0.027	1
Image 6	63.07	0.032	1
Image 7	62.04	0.040	1

III. CONCLUSION

In this paper, the proposed steganographic model was tested on seven different medical images. These medical images were shown to the different person for analyzing the change between original and the image having information. And the results shows that when we use Gray Level Modification Method, the imperceptibility of the medical images was not effected as the change in the image pixel is only +1 and -1 i.e. MAXERR=1. This change does not identify by the normal HVS (Human Visualization System). These seven images were also tested on the PSNR and MSE and obtained good results as shown in the above tables. This model may decrease the paper work in medical system and may also be used in other areas like Geographical Information System in satellite imaging etc.

IV. REFERENCES

[1] Jichkar, Samiksha K., and Mahip M. Bartere, (2015). A Comparative Study of Various image Steganographic Techniques Used for Information Hiding."Compusoft 4.5 1730.

[2] Gutub, A. A. A. (2010). Pixel indicator technique for RGB image steganography. Journal of Emerging Technologies in Web Intelligence, 2(1), 56–64. http://doi.org/10.4304/jetwi.2.1.56-64

[3] Liang, G. L., Wang, S. Z., & Zhang, X. P. (2007). Steganography in binary image by checking data-carrying eligibility of boundary pixels. Journal of Shanghai University, 11(3), 272–277. http://doi.org/10.1007/s11741-007-0317-2

[4] Pal, A., & Pramanik, T. (2013). Design of an Edge Detection Based Image Steganography with High Embedding Capacity. Quality, Reliability, Security and Robustness in …, 794–800. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-37949-9_69

[5] Modi, M. R., Islam, S., & Gupta, P. (2013). Edge based steganography on colored images. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7995 LNCS, 593–600. http://doi.org/10.1007/978-3-642-39479-9_69

[6] Jia-Fa, M., Xin-Xin, N., Gang, X., Wei-Guo, S., & Na-Na, Z. (2015). A steganalysis method in the DCT domain. Multimedia Tools and Applications, (180). http://doi.org/10.1007/s11042-015-2708-0

[7] M.M., S., G., S., & S.H., S. (2015). Detection of rapid eye movement behaviour disorder using short time frequency analysis of PSD approach applied on EEG signal (ROC-LOC). Biomedical Research (India), 26(3), 587–593.

[8] Chen, P., & Lin, H. (2006). A DWT Based Approach for Image Steganography, (4), 275–290.

[9] Al-taani, A. T., Al-issa, A. M., & Steganograhy, A. O. (2009). A Novel Steganographic Method for Gray-Level Images. Engineering, 3(3), 5–10.

[10] Puech, W. (2008). Image encryption and compression for medical image security. 2008 1st International Workshops on Image Processing Theory, Tools and Applications, IPTA 2008, 1–3. http://doi.org/10.1109/IPTA.2008.4743800

[11] Al-Dmour(B) and Al-Ani, A Medical Image Steganography Method Based on Integer Wavelet Transform and Overlapping Edge Detection, ICONIP 2015, Part IV, LNCS 9492, pp. 436–444, 2015. DOI: 10.1007/978-3-319-26561-2 52

[12] Jain, M., & Lenka, S. K. (2016). Diagonal queue medical image steganography with Rabin cryptosystem. Brain Informatics, 3(1), 39–51. http://doi.org/10.1007/s40708-016-0032-8

[13] Liu, J., Tang, G., & Sun, Y. (2013). A secure steganography for privacy protection in healthcare system. Journal of Medical Systems, 37(2). http://doi.org/10.1007/s10916-012-9918-z

[14] Rao, N. V., & Kumari, V. M. (2011). Watermarking in Medical Imaging for Security and Authentication. Information Security Journal: A Global Perspective, 20(3), 148–155. http://doi.org/10.1080/19393555.2011.561154Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .