A Comparative Study between LSB and Modified Bit Replacement (MBR) Watermarking Technique in Spatial Domain for Biomedical Image Security

Koushik Pal

Institute of Radio Physics and
Electronics, University of
Calcutta, Kolkata, 700009,
India

Goutam Ghosh

Institute of Radio Physics and
Electronics, University of
Calcutta, Kolkata, 700009,
India

Mahua Bhattacharya

Indian Institute of Information
Technology and Management,
Gwalior, 474010, India

Abstract: The current paper proposes a biomedical image watermarking technique through modified bit replacement algorithm in spatial domain. In this algorithm, multiple copies of the same information are hidden in the biomedical images. Detection is performed by applying bit majority algorithm which can reconstruct the hidden information from different recovered sets subjected to some common attacks. Keys for watermark recovery are also embedded in the cover image. The superiority of the proposed modified bit replacement scheme over the LSB technique is indicated through evaluation of image quality metrics that shows much enhancement in the visual and statistical invisibility of hidden data.

Keywords: Biomedical image watermarking, spatial domain, data security, image quality metrics.

1. INTRODUCTION

The rapid growth and advancement of digital networks and multimedia technologies has created immense interest in the areas of tele-diagnosis tele-medicine, tele-radiology, tele-surgery and remote patient monitoring. The digitization of patient information, such as electronic patient records (EPR), clinical and diagnostic images, has provided significant flexibility and more accuracy in medical diagnosis. Patient records are required to be secure and information confidentiality maintained. For biomedical images, modifications are not allowed during data transfer over networks for obvious legal reasons. Digital watermarking can embed messages without changing the image size and without violating the DICOM format maintaining the following necessary conditions:

- I. There should be minimal perceptible changes in the watermarked image. The watermarked image should visually be the same as the original image [1].
- II. The watermarking technique should be reversible. This means that the watermarked image should revert back to its original form on removal of the water mark [2].
- III. There should be no impact on the stored images in the PACS server due to introduction of the watermark [3].
- IV. Modification of the watermarked image may lead to unsuccessful verification. So the proposed watermarking scheme should not change the amount of data that needs to be transferred.
- V. The watermarking technique for authentication should be applied while transferring image data in DICOM format over the network [4].

Digital watermarking is one of the safest and popular methods to enhance medical data security [5]. It is the process of embedding information into a digital image with an imperceptible form for the human visual system such that the hidden information or the watermark can be extracted or recovered afterwards [6-9]. However, medical image watermarking requires extreme care when embedding additional information because the additional information should not degrade the medical image quality.

If a medical image is illegally obtained and the content is changed, it may lead to wrong diagnosis. Watermarking of medical images and authentication of legal documents face extremely hostile environments where the most harmful attacks remove the embedded watermarks [10, 11].

A biomedical image watermarking technique can be characterized by the following four features: imperceptibility, robustness, security, and capacity.

Imperceptibility: Imperceptibility refers to the perceptual transparency of the watermark. Ideally, no perceptible difference between the watermarked and original image should be perceived by the human visual system.

Robustness: Robustness is the capability of the watermark to survive unwanted alterations or manipulations known as attacks. A watermark needs only to survive the attacks that are likely to occur when the watermarked signal is being transmitted. Not all watermarking applications require a watermark to be robust enough to survive all attacks. In an extreme case, robustness may be completely irrelevant where fragility is desirable [12].

Security: Watermarking security implies that the watermark should be difficult to remove or alter without damaging the

host image. It is the most important figure of merit for a medical image assuring secrecy and integrity of the watermarked information [13].

Capacity: Watermarking capacity normally refers to the amount of information that can be embedded into the cover image [14].

Watermarks can be applied in the spatial domain or in the frequency domain. Spatial domain techniques, such as the least significant bit method, embed the message by altering the coefficients of the least significant bit of an image. The frequency domain technique embeds the message by modulating the coefficients in the frequency domain, such as in the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) cases. Both domains have their own advantages and disadvantages. Since frequency domain techniques can embed more bits of information and provide ease of compression it is more commonly used. Spatial domain techniques are simple but suffer from the disadvantage that they are not robust enough to overcome several attacks or image alterations.

In this paper the proposed watermarking technique is compared with the simple LSB technique using several image quality metrics that show that the superiority of the proposed algorithm over the latter in terms of authenticity and integrity of DICOM images. Further, the embedded watermark or information logo can be recovered using this algorithm which resembles the hidden image more closely.

2. WATERMARKING USING SIMPLE LSB TECHNIQUE IN SPATIAL DOMAIN

The Least Significant Bit (LSB) algorithm, is very simple, strong, and less perceptible. The embedding of the watermark is performed choosing a subset of image pixels and substituting the LSB of each of the chosen pixels with the watermark bits [15]. This algorithm takes as inputs a cover image and a watermark logo while the output function takes as input the watermarked image and gives the extracted watermark as its output. For a gray scale 8-bit image, we need to read the cover image and information logo and then add the data of the information logo to the least significant bits of each pixel of the cover image, in every 8-bit pixel. The cover image is generally a gray scale image where each pixel is represented by 1 byte. It can represent 256 gray colors between the black which is 0 to the white which is 255. The information logo is generally a binary image and it can be represented by black (0) or white (1). Recovery of the hidden information or watermark is done by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the watermark is reconstructed.

Though LSB watermarking schemes have a higher level of invisibility and a less computational overhead, modifications of LSB data is highly sensitive to noise and is easily destroyed. This technique is not resistant enough to image compression and other image processing techniques. Furthermore, image quality may be degraded by the watermark.

This paper describes a new type of biomedical image watermarking technique which is also simple but more effective and efficient than the LSB technique.

3. PROPOSED WATERMARKING TECHNIQUE IN SPATIAL DOMAIN

In the proposed biomedical image watermarking technique, modified bit replacement algorithm in spatial domain is used which is much better than the conventional simple LSB technique. In this scheme, multiple copies of the same information are hidden in several bits of the cover image starting from the lower order to the higher orders. So even if some of the information is lost due to an attack, we can still collect the remaining information and recover the watermark from the cover image using the bit majority algorithm.

3.1. Embedding watermark

The gray scale cover image is divided into several parts according to the size of the information logo and the number of the same information that are to be hidden. Then the lowest pixel value of each sub division is taken as the starting index for the embedding process and this value gradually increases up to the limit equal to the maximum number of information blocks of the watermark. The number of information blocks is the total number of black pixels of the binary logo. This number is also used as a random key which is also sent along with the watermarked image and two other keys which hold the information about the dimensions of the watermark.

3.2. Recovery of watermark

The watermarked image is compared with the original cover image to find the difference in pixel values depending on the three hidden keys. The first key indicates the information block of the information logo and the remaining two indicate the row size and column size of the information block respectively. After getting the three correct keys from the user the different hidden sets of information logo from the watermarked image are found. These different sets are built using the positional information of the hidden pixels and the information obtained from those three keys. The final information logo is then reconstructed by a number of comparisons between these different recovered sets using the proposed bit majority algorithm. This algorithm provides a method to find the closest twin by several comparisons between different sets of data. After recovering the different sets from the attacked watermarked image, the best sets of pixels which are closest to the original information logo, are taken. The rest of the portions of black dots are replaced by white dots. Every set of the recovered logo is checked with one another to find the similarity between the pixels.

4. ATTACKS AND DISTORTIONS

Alterations on the watermarked image made either intentionally or inadvertently, are known as attacks. Different types of attacks can cause image quality degradation. An attack may be performed intentionally on a watermarked document to destroy or degrade the quality of the hidden watermark. These distortions also introduce degradation on the performance of the watermark extraction algorithm [16]. The watermarking technique should be robust enough to survive the attacks so that after extraction the watermark should resemble the original image. Some of the popular attacks mentioned in this paper are (a) *Salt and Pepper Noise*, (b) *Image Compression*, (c) *Gaussian Noise*, (d) *Multiplicative Noise* and (e) *Erosion*.

5. IMAGE QUALITY METRICS

Measurement of the quality of a watermarked image and the recovered information logo is very important for the

watermarking technique to indicate its strength and integrity [17, 18].

To measure the amount of visual quality degradation between the original and watermarked images, different types of image quality metrics such as Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measurement (SSIM), Bit Error Rate (BER), Normalized Absolute Error (NAE), Mean Average Error (MAE), Universal Image Quality Index (UIQI) are used while the quality and similarity of the recovered information logo with the original may be measured by determining the BER, SSIM, Normalized Cross Correlation (NCC), Mutual Information (MI), Structural Content (SC), and UIQI.

Higher value of PSNR, SSIM, NCC, MI and UIQI represents image of good quality while lower values of BER, NAE, MAE, SC represent less error and consequently good quality image

6. RESULTS AND DISCUSSION

A comparative study of the quality measurements between the simple LSB watermarking technique and the proposed modified bit replacement (MBR) watermarking technique has been calculated and the results are presented.

In Table 1, four sets of biomedical cover images along with the information logos and the obtained watermarked images are shown for both the LSB and our proposed embedding technique. The calculated value of the quality metrics such as PSNR, SSIM, UIQI, BER, MAE and NAE are given to find the image quality after watermark insertion. It is observed that for both the cases the difference between the watermarked image and the cover image by the Human Visual System appear to be identical. In case of the LSB technique we are hiding a single logo but in case of our proposed algorithm we are hiding 8 sets of information logo. So, the chance of deformity of the original image is more in the proposed case. But from Table 1 we observe that the value of SSIM in all the cases of the proposed algorithm is close to 1 and BER is close to 0 which are proof of the similarity between the original and watermarked cover image. The values of the other quality metrics also indicate that the watermarked images are quite similar to the original cover images without any distortions or visual deformities. The value of universal image quality index (UIQI) is also close to 1 which is proof of the good quality of the watermarked image.

In Table 2 through Table 6, the successful recovery of hidden information from the altered watermarked image is shown under several attacks for both the simple LSB and proposed biomedical watermarking. The results are shown for some biomedical MRI images subjected to different types of attacks such as salt and pepper noise, image compression, Gaussian noise, multiplicative noise, erosion and dilation. The recovered logos are visually more similar to the original one in our proposed MBR technique than the LSB technique. Moreover, from the experimental results we can see our proposed technique can resist higher order of attack and still can recover the hidden information whereas the simple LSB technique fails to recover and construct the hidden information in such circumstances. The values of SSIM and BER of the recovered logo using MBR technique indicate that they are much closer to the embedded one and also much better than LSB technique. Moreover NCC and UIQI also prove the quality of the recovered watermark or information logo. In comparison with the LSB and our proposed MBR watermarking technique BER and SC are less and closer to 0. SSIM, NCC, MI and UIQI are higher and closer to 1.

From Table 2 we can see our proposed watermarking technique can recover the watermark more close to the original one than LSB under 40 % of salt and pepper noise. From Table 3 we can see that LSB technique cannot resist JPEG compression whereas the proposed technique can recover information closer to the hidden one from 5 % JPEG compressed image. Results from Table 4 describe that the proposed algorithm is much stronger to recover hidden information from Gaussian noise attack than the LSB technique. Other tables also show that the proposed MBR biomedical image watermarking technique is quite efficient to recover information from other attacked watermarked image like multiplicative noise and erosion.

The value of different quality metrics mentioned in Table 1 to Table 6 indicates that the proposed modified bit replacement (MBR) biomedical watermarking technique is much better both visually and statistically than the simple and conventional LSB watermarking technique.

7. CONCLUSION

The proposed MBR biomedical image watermarking scheme in the spatial domain includes procedures for data embedding, extraction and verification of quality using several quality metrics for both watermarked image and the recovered watermark. Experimental results show that the proposed modified bit replacement watermarking scheme has high robustness, embedding capacity, low distortion and enhanced security than the LSB technique. Moreover it can also resist several moderately strong attacks. It is also observed that the original information logo can be reconstructed by the proposed bit majority algorithm whose integrity can be strictly verified. A number of image quality metrics support the quality, strength and satisfy the high performance of the proposed algorithm.

8. ACKNOWLEDGMENTS

It is my pleasure to express my heartiest thanks to all the faculty members of Institute of Radio Physics and Electronics, University of Calcutta, Kolkata and the Electronics and Communication Engineering Department of Guru Nanak Institute of Technology, Kolkata for their ungrudging support and cooperation.

9. REFERENCES

- [1] Fazli, S. and Khodaverdi, G, Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics, 2010, IEEE DOI 10.1109/ICMV.2009.68
- [2] Siau-Chuin Liew; Zain, J.M., "Reversible medical image watermarking for tamper detection and recovery", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 5, pp. 417-420, 2010.
- [3] Cao, F., Huang, H.K. & Zhou, X.Q., "Medical image security in a HIPAA mandated PACS environment", Computerized Medical Imaging and Graphics, vol. 27, no. 2- 3, pp. 185-196, 2003.
- [4] Kobayashi, L.O.M.; Furuie, S.S.; Barreto, P.S.L.M., "Providing Integrity and Authenticity in DICOM Images: A Novel Approach, IEEE Transactions on Information Technology in Biomedicine," vol. 13, Issue: 4, pp. 582-589, 2009.
- [5] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorrec, "Relevance of Watermarking in Medical Imaging", in Proceedings of the IEEE EMBS Conf. on

- Information Technology Applications in Biomedicine, Arlington, USA, Nov., pp. 250-255, 2000.
- [6] "Digital Image Processing Using MATLAB", 2nd edition, by Gonzalez, Woods, and Eddins, Gatesmark Publishing, ISBN 9780982085400.
- [7] Miller, M.L., Cox, I.J., Linnartz, J.M.G. & Kalker, T., "A Review of Watermarking Principles and Practices" in Digital Signal Processing for Multimedia Systems, eds. K.K. parhi & T. Nishitani, Marcel Dekker Inc., New York, 1999.
- [8] G. Langelaar, I. Setyawan, and R. Lagendijk. Watermarking digital image and video data. IEEE Signal Processing Magazine, vol. 17, pp. 20-46, 2000.
- [9] C. Podilchuk and E. Delp. Digital Watermarking Algorithms and Applications. In IEEE Signal Processing Magazine, vol. 18, no. 4, July 2001.
- [10] Zain, J.M.; Fauzi, A.R.M., "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)", 29th Annual International Conference of the IEEE on Engineering in Medicine and Biology Society, EMBS 2007. pp. 5661-5664, 2007.
- [11] Velumani, R.; Seenivasagam, V., "A reversible blind medical image watermarking scheme for patient identification, improved telediagnosis and tamper detection with a facial image watermark", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-8, 2010.
- [12] C. Rey and J.L. Dugelay. A survey of watermarking algorithms for image authentication. EURASIP Journal on Applied Signal Processing, vol. 6, pp.613–621, 2002.
- [13] H-M. Zhao, C-M. Hsu, and S-G Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," IEEE Trans. Information Technology in Biomedicine, vol. 6, pp. 46-53, 2002.
- [14] Tian, J. 2003, "High capacity reversible data embedding and content authentication", IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 517- 520, 2003.
- [15] Lee, G. J., Yoon, E. J. and Yoo, K. Y., "A new LSB based Digital Watermarking Scheme with Random Mapping Function", 2008, IEEE DOI 10.1109/UMC.2008.33
- [16] Huang, H.; Coatrieux, G.; Shu, H.Z.; Luo, L.M.; Roux, C., Medical image integrity control and forensics based on watermarking - Approximating local modifications and identifying global image alterations. "Annual International Conference of the IEEE on Engineering in Medicine and Biology Society, EMBC, pp. 8062-8065, 2011.
- [17] M. Eskicioglu and P. S. Fisher, "Image Quality Measures and Their Performance," *IEEE Transactions on Communications*, vol. 43, no. 12, pp. 2959-2965, December 1995.
- [18] H. R. Sheikh, M. F. Sabir and A. C. Bovik, "A Statistical Evaluation of Recent Full Reference Image Quality assessment Algorithms," IEEE Transactions on image processing, vol. 15, no. 11, pp. 3441-3456, November 2006.

Table 1: Cover Image, watermark or information logo and image quality measurements for both LSB and MBR algorithm

	Cover Image	Information Logo	Watermarking Technique	watermarked image	Image quality measures		
					PSNR	SSIM	UIQI
SET 1		S Logo	Simple LSB		51.17	0.99556	0.93536
					BER	MAE	NAE
					0.49568	0.496	0.00977
		No of Information Block 93	Proposed MBR		PSNR	SSIM	UIQI
					42.29	0.97293	0.90468
					BER	MAE	NAE
SET 2		E Logo	Simple LSB		PSNR	SSIM	UIQI
					51.1624	0.99757	0.98506
					BER	MAE	NAE
		No of Information Block 140	Proposed MBR		0.49754	0.498	0.00849
					PSNR	SSIM	UIQI
					40.5349	0.98105	0.96866
SET 3		B Logo	Simple LSB		PSNR	SSIM	UIQI
					51.1823	0.99505	0.76853
					BER	MAE	NAE
		No of Information Block 130	Proposed MBR		0.49527	0.495	0.00785
					PSNR	SSIM	UIQI
					40.8229	0.96193	0.84927
SET 4		KP Logo	Simple LSB		PSNR	SSIM	UIQI
					51.0685	0.99536	0.71935
					BER	MAE	NAE
		No of Information Block 109	Proposed MBR		0.50842	0.508	0.01058
					PSNR	SSIM	UIQI
					41.2924	0.97498	0.86849
	Brain MRI (Top View)				BER	MAE	NAE
					0.05563	0.42175	0.00878

Table 2: Watermarked image, salt and pepper noise attacked watermarked image, recovered logo and image quality measures

Recovery Technique	Watermarked Image	Amount of attack	Noisy image	PSNR	Original and Recovered logo	Image quality measures		
Simple LSB		20%		10.99		BER	SSIM	NCC
						0.44531	0.06346	0.5714
					MI	SC	UIQI
						0.00759	1.08889	0.0737
Proposed MBR		20%		10.98		BER	SSIM	NCC
						0.00391	0.99683	1.0000
					MI	SC	UIQI
						0.95027	0.99324	0.9922
Simple LSB		30%		9.24		BER	SSIM	NCC
						0.34766	0.22800	0.6428
					MI	SC	UIQI
						0.06792	1.00800	0.2558
Proposed MBR		30%		9.24		BER	SSIM	NCC
						0.03906	0.91396	0.9841
					MI	SC	UIQI
						0.77205	0.95455	0.8965
Simple LSB		40%		8.29		BER	SSIM	NCC
						1.00000	0.11482	0.7500
					MI	SC	UIQI
						0.09113	0.86740	0.1648
Proposed MBR		40%		8.28		BER	SSIM	NCC
						0.14453	0.65472	0.9139
					MI	SC	UIQI
						0.43845	0.88520	0.6596

Table 3: Watermarked image, JPEG Compression attacked watermarked image, recovered logo and image quality measures

Recovery Technique	Watermarked Image	Amount of attack	Noisy image	PSNR	Original and Recovered logo	Image quality measures for recovered logo		
Simple LSB		2%		50.43		BER	SSIM	NCC
						0.42578	0.18787	0.6258
					MI	SC	UIQI
						0.01224	1.0068	0.1333
Proposed MBR		2%		54.90		BER	SSIM	NCC
						0.00000	1.00000	1.0000
					MI	SC	UIQI
						0.98405	1.0000	1.0000
Simple LSB		3%		52.01		BER	SSIM	NCC
						0.43359	-0.0208	0.5317
					MI	SC	UIQI
						0.01261	1.05882	0.0377
Proposed MBR		3%		40.46		BER	SSIM	NCC
						0.05469	0.80754	0.9603
					MI	SC	UIQI
						0.69693	0.96923	0.8320
Simple LSB		5%		52.09		BER	SSIM	NCC
						0.36328	0.10754	0.6977
					MI	SC	UIQI
						0.05603	1.04484	0.1705
Proposed MBR		5%		41.92		BER	SSIM	NCC
						0.06250	0.87479	0.9698
					MI	SC	UIQI
						0.66550	0.96399	0.8668

Table 4: Watermarked image, Gaussian Noise attacked watermarked image, recovered logo and image quality measures

Recovery Technique	Watermarked Image	Noisy image	PSNR	Original and Recovered logo	Image quality measures		
Simple LSB			46.78		BER	SSIM	NCC
					0.46875	-0.1071	0.5782
				MI	SC	UIQI
					0.00152	1.02797	-0.026
Proposed MBR			49.09		BER	SSIM	NCC
					0.02344	0.95255	0.9863
				MI	SC	UIQI
					0.82424	0.98658	0.9516
Simple LSB			49.15		BER	SSIM	NCC
					0.47656	-0.0432	0.4841
				MI	SC	UIQI
					0.00151	1.0678	-0.013
Proposed MBR			40.18		BER	SSIM	NCC
					0.00391	0.95005	1.0000
				MI	SC	UIQI
					0.96691	0.99213	0.9755
Simple LSB			49.21		BER	SSIM	NCC
					0.50781	0.07570	0.4398
				MI	SC	UIQI
					0.00704	0.99966	-0.019
Proposed MBR			40.02		BER	SSIM	NCC
					0.05469	0.93935	0.9570
				MI	SC	UIQI
					0.72331	0.98272	0.9253

Table 5: Watermarked image, Multiplicative noise attacked watermarked image, recovered logo and image quality measures

Recovery Technique	Watermarked Image	Noisy image	PSNR	Original and Recovered logo	Image quality measures		
Simple LSB			43.70		BER	SSIM	NCC
					0.3984	0.19705	0.6530
					MI	SC	UIQI
					0.02476	1	0.1786
Proposed MBR			46.55		BER	SSIM	NCC
					0.01953	0.98918	0.9863
				MI	SC	UIQI
					0.84527	0.99324	0.9702
Simple LSB			42.33		BER	SSIM	NCC
					0.30859	0.29201	0.7222
				MI	SC	UIQI
					0.10942	0.93333	0.3486
Proposed MBR			39.24		BER	SSIM	NCC
					0.04688	0.90073	0.9682
				MI	SC	UIQI
					0.73051	0.96923	0.8869
Simple LSB			35.35		BER	SSIM	NCC
					0.24609	0.66567	0.7964
				MI	SC	UIQI
					0.19081	1.0315	0.5811
Proposed MBR			34.59		BER	SSIM	NCC
					0.03516	0.83182	0.9820
				MI	SC	UIQI
					0.78671	0.99356	0.9100

Table 6: Watermarked image, attacked watermarked image due to Erosion, recovered logo and image quality measures

Recovery Technique	Watermarked Image	Noisy image	PSNR	Original and Recovered logo	Image quality measures		
Simple LSB			20.53		BER	SSIM	NCC
					0.42188	0.09947	0.4081
				MI	SC	UIQI
					0.03924	1.81481	0.1443
Proposed MBR			20.49		BER	SSIM	NCC
					0.08594	0.71682	0.9659
				MI	SC	UIQI
					0.56838	0.92453	0.8182
Simple LSB			18.49		BER	SSIM	NCC
					0.39453	0.27367	0.5158
				MI	SC	UIQI
					0.03255	1.2000	0.2476
Proposed MBR			18.47		BER	SSIM	NCC
					0.11328	0.81104	0.9285
				MI	SC	UIQI
					0.49918	0.91971	0.7771
Simple LSB			22.39		BER	SSIM	NCC
					0.29688	0.46485	0.7471
				MI	SC	UIQI
					0.12279	1.0448	0.4149
Proposed MBR			22.37		BER	SSIM	NCC
					0.10547	0.67195	0.9450
				MI	SC	UIQI
					0.49788	0.95829	0.7452