International Journal of Biotechnology and Biomedical Sciences
p-ISSN 2454-4582, e-ISSN 2454-7808, Volume 5, Issue 1; January-June, 2019 pp. 53-56

http://www.krishisanskriti.org

Robust and Secure Medical Image Watermarking for Bioinformatics Applications

Dr. Harsh Vikram Singh[2] and Kumari Suniti Singh[1]

[1]*Associate Professor, Department of Electronics Engineering, Kamla Nehru Institute of Technology, Sultanpur (India)*
[2]*Research Scholar, Department of Electronics Engineering, Kamla Nehru Institute of Technology, Sultanpur (India)*

Abstract—*In this paper, we discussed the role of the watermarking technique used in medical image security i.e. to maintain its integrity, authenticity, confidentiality, reliability, etc. The authenticity and integrity of a medical image is a critical topic of research now a day used in e-health services. Watermarking has found an important role in securing medical images.*

Keywords*: Medical images, security, digital watermarking, Cryptography.*

I. INTRODUCTION

Watermarking is the most commonly and frequently used technique in telemedicine. Now a day's many hospitals and an e-health care centers use hospital information system (HIS), radiology information system (RIS), picture archiving and communication system (PACS) and many others technologies [1][2]. The use of such systems provides the sharing of medical data and electronics patient records (EPR) to the remote areas for medical diagnosis [1]. Instead of this advancement in telemedicine, teleradiology and teletaurmacare, it is easy to intercept and tamper medical images in transmission over a public network. So it is very necessary to provide a secured form of transmission. The confidentiality, authenticity and integrity of medical image must be fulfilled [1][3]. Confidentiality ensures that only desired users can assess the transmitted image, authenticity ensures that image is related to the claimed patient and also comes from the required source, integrity provides that there is no modification has been done in the image [1][3]. Presently cryptography and watermarking are mostly used to provide the security of data. Both also fulfil the security requirements of the medical image. Cryptography uses digital signatures, hashing and encryption of image, whereas watermarking provides robust and fragile watermarks [4] [5]. The drawback of cryptography is that any kind of loss and deletion of attached data makes the image corrupt. So it is difficult to verify its integrity and authenticity. Whereas watermarking provides robust and fragile watermarks to secure the data [3][6]. Crypto-watermarking is used to utilize the benefits of both cryptography and watermarking techniques. Different types of crypto-watermarking algorithms are available to provide security for exchanging medical images. The crypto-watermarking can be methods can be classified as irreversible methods, reversible methods and region based methods [1]. The irreversible watermarking is lossy and may provide permanent alterations to the image. Reversible watermarks provide lossless image after extraction of the watermark. Region-based watermarking basically provides segmentation of the original image into two categories that are the region of interest (ROI) and region of non- interest (RONI). Embedding is done using either reversible or irreversible watermarking [7] [8].

This paper is sorted out as follows:

Section I. Introduction. Section II. Digital watermarking of medical images. Section III. Techniques of watermarking used for medical images. Section IV. Performance Evaluation Parameters. Section V. Conclusion

II. Digital watermarking of medical images

Watermarking is mainly utilized for copyright protection and verification of image. It is created in such a way that the image is recognizable. Digital watermarking is a procedure that allows the addition of information in the form of the watermark into the object. Watermarks are embedded in the object by using watermark embedder, now and then it depends on curtain embedding key. On the other end Watermark detector is used for detecting the predefined watermark present in the object. When used in specified application digital watermarking deals with two issues i.e. address security (i.e. authenticity, integrity and confidentiality) and system consideration (i.e. memory and bandwidth saving, to avoid detachment) [6]. Data hiding is the fundamental and main property of watermarking [9]. The confidentiality is kept by concealing the information into the picture. The hiding property of data provided by watermarking also eliminates detachment. More and more medicinal images are being created and used using radiology around the globe, which provides information to medical researchers, medical

practicing and students [10]. Also choices of design and evaluation parameters are also necessary to apply a proper watermarking technique. Design parameters give how to characterize the development of a watermarking technique and evaluation parameter shows the level of performance of a watermarking technique [6]. Typically used parameters for generation of watermarking and embedding are visibility, the capacity of embedding, imperceptibility etc. similarly robustness, invertibility and error probability are the parameters used for detection [11].

III. Techniques of watermarking used for medical images

Now a day's digital watermarking is a broad area of research and frequently used in medical image security. It is easily available and protects the data in an efficient manner. Watermarking can be done in two ways either in the spatial domain or in the frequency domain [12]. In the spatial domain, the watermark is performed by adjustment of pixel values, whereas in transform domain watermark is applied in the transformed coefficients. There are various types of transform domain techniques are available such as Discrete cosine transform (DCT), Discrete wavelet transform (DWT), Discrete Fourier transform (DFT) etc. Transform domain techniques are most commonly used compare to the spatial domain because of its robustness.

(A) Watermarking using Spatial domain

Images basically contain pixels. So in spatial domain watermark is embedded in some specific pixels of image [13]. At the time of watermark extraction, watermark has been extracted from those specific pixels. Spatial domain technique can be easily used and takes less time however unable to face various types of attacks during transmission [12].

(B) Watermarking using transform domain

Transform domain watermarking provides good result compare to spatial domain watermarking. In this technique watermarking firstly image is converted using appropriate transform domain technique after that embedding of watermark has been done in the transform coefficients. At the end inverse transform has been done to get a watermarked image. Generally utilized transform domain techniques are DCT, DWT and DFT etc. [14].

a) Discrete Fourier Transform

Most of the information of an image is available in Phase and its magnitude coefficients and since DFT gives a complex valued function so it provides both phase and magnitude information. It also provides robustness against geometric attacks (i.e. translation, scaling and cropping etc.). The DFT magnitude domain watermarking also provides translational-invariance. DFT embedding should be possible in two different form i.e. direct embedding and the template based embedding [12]. In direct embedding phase and magnitude coefficients have been modified and then the watermark embedding is done.

b) Discrete Cosine Transform

DCT transform is suitable to give grey-scale images. In this the requirement to access the non-marked images in detection level is eliminated, thus it gives a better result when the comparison between watermarked and original image done. Though in this process it losses some robustness [15]. In this, the watermark contains pseudo-random sequence which superimposes to some of the coefficients of DCT transform [15]. Embedding is done by dividing the image into non-overlapping 8*8 blocks. Then calculating the forward DCT of each non-covering block using HVS block selection method and using the highest coefficient selection criteria [12][16]. Finally, embedding of watermark has been performed on selected coefficients and taking inverse DCT of each block.

c) Discrete Wavelet Transform

DWT provides a multi-resolution characteristics of an image i.e. it is able to analyze the image at multiple resolutions. When DWT is performed on an image it decomposes it into two components that is high-frequency components (detail coefficients i.e. LH, HL, HH) and low-frequency component (approximation coefficient i.e. LL). Decomposition is repeated until the entire images have been decomposed [17]. The detail of the original images contained in low-frequency coefficients i.e. LL, so the watermark is embedded in the LL coefficients. After applying IDWT original image can be reconstructed from decomposed one [18].

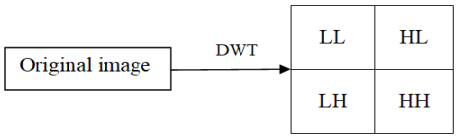

Fig. 1: DWT Level 1 decomposition of the image

IV. Performance Evaluation Parameters

Performance of watermarking technique can be evaluated utilizing various parameters for example MSE, PSNR, SNR, BER, SSIM and Accuracy Ratio etc.

Mean Square Error (MSE): It is given by the average squared difference between the original and distorted image. MSE can be calculated by the formula [18][19].

$$MSE = \frac{\sum_{i,j}(I\ (i,j) - I_w(i,j))^2}{M * N}$$

Peak Signal to Noise Ratio (PSNR): It gives the measure of quality between the Original and Watermarked image. It can be given as [12][18]

$$PSNR = 10log_{10}\frac{(R^2)}{MSE}$$

Where R is the highest value of the image. For 8 bit image R= 255.

Signal to Noise Ratio: It shows the sensitivity measure of the image. It can be calculated as [12],

$$SNR_{db} = 10 \log \frac{P_{signal}}{P_{noise}}$$

Bit Error Rate (BER): It provides the comparison between bit values of the original image and watermarked image [12]. Lower the bit error rate, higher the efficiency [18]. BER is given as,

$$BER = C/(H * W)$$

where H and W show the height and width of the watermarked image respectively. C shows the number of count. The starting value will be zero and if any difference of bits occurs between the original and watermarked image the value of C increases.

Accuracy Ratio: It is used to calculate the relation between original watermarked bit and correct bits and can be given as [18],

$$AR = \frac{CB}{NB}$$

Where CB shows correct bits and NB shows a number of bits of the original watermarked image.

Structural Similarity Index (SSIM): It represents the nature of the image by giving the demographic changes between the original and watermarked image. It is given as [18][20],

$$SSIM(I, I_w) = \frac{(2\mu_1\mu_{1w}+C_1)(2cov+C_2)}{(\mu_1^2+\mu_{1w}^2+C_1)(\sigma_1^2+\sigma_{1w}^2+C_2)}$$

where c_1 and c_2 are the constants. Its values are $c_1 = (0.01 * R)$ and $c_2 = (0.03 * R)$, R is dynamic range and its value is 255 for 8-bit the grayscale image.

V. CONCLUSION

Digital watermarking is an extremely valuable technique utilized in information security and authentication of data. However, watermarking of medical image is very important nowadays to protect the data from tampering and any kind of attacks during transmission. There is a need for efficient and strong techniques for utilizing in different medical administration. In this paper, we have talked about watermarking techniques such as spatial domain and transform domain methods such as DCT, DWT and DFT. Also it is required to choose an appropriate watermarking technique for different applications and according to need. So digital watermarking is an ongoing and emerging technique in the field of image security.

REFERENCES

[1] Ali Al-Haj, Ahmad Mohammad & Alaa Amer "Crypto-Watermarking of Transmitted Medical Images", Society for Imaging Informatics in Medicine, DOI 10.1007/s10278-016-9901-1, 2016.

[2] Huang HK, "PACS and imaging informatics, basic principles and applications", Wiley-Blackwell, New York, ISBN: 978-0-470-37372-9, 2010.

[3] Ali Al-Haj & Alaa Amer, "Secured Telemedicine Using Region-Based Watermarking with Tamper Localization", Society for Imaging Informatics in Medicine, DOI 10.1007/s10278-014-9709-9, 2014.

[4] Kobayashi L, Furuie S, Barreto P, "Providing integrity and authenticity in DICOM images: a novel approach", IEEE Trans. Inf. Technol. Biomed., Vol. 13, Issue 4, pp. 582–589, 2009.

[5] Rodrigues JM, Puech W, Fiorio C, "Lossless crypto-data hiding in medical images without increasing the original image size", 2nd Int. Conf. Adv. Med. Signal Inf. Process, pp. 358–365, Sep. 2004,

[6] Nyeem H, Boles W, Boyd C: A review of medical image watermarking requirements for teleradiology. J Digit Imaging 26(2), pp. 326–343, 2012.

[7] Wu J, et al., "Tamper detection and recovery for medical images using near-lossless information hiding technique", J Digit Imaging 21, pp. 59–76, 2008.

[8] Chiang K, Chang K, Chang R, Yen H, "Tamper detection and restoring system for medical images using wavelet-based reversible data embedding", J Digit Imaging 21, pp.77–90, 2008.

[9] Fallahpour M, Megias D, Ghanbari M: High capacity, reversible data hiding in medical images. In: Image processing (ICIP), 16th IEEE International Conference on, pp. 4241–4244, 2009.

[10] Das S, Kundu M, "Effective management of medical information through a novel blind watermarking technique", Journal of Medical Systems, pp. 1–13, 2009.

[11] Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T: Models of watermarking. In: Digital watermarking and steganography (second edition), Burlington: Morgan Kaufmann, ISBN 978-0-12-372585-1, pp. 61–103, 2008.

[12] S. Tyagi, H. V. Singh, R. Agarwal and S. K. Gangwar, "Digital Watermarking Techniques for Security Applications", International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems, IEEE 978-1-5090-2118-5/16, 2016.

[13] N. Chandrakar and J. Baggaa, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of Computer Application Technology and Research, vol. 2, no. 2, pp. 126-130, 2013.

[14] F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes", Pattern Recognition Letter, 2013.

[15] M. Barni, F. Bartolini, V. Cappellini, A. Piva, "A DCT-domain system for robust image watermarking", Signal Processing 66, pp.357-372, 1998.

[16] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN), **ISBN:** 0-7803-9094-6, 2005.

[17] A. F. Qasima, F. Mezianea, R. Aspina, "Digital watermarking: Applicability for developing trust in medical imaging work flows state of the art review", Elsevier Computer Science Review 27, pp. 45–60, 2018.

[18] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, 2013.

[19] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, ―A Novel Technique for Digital Image Watermarking in Spatial Domain, 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.

[20] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity", IEEE Trans. Image Process. 13, pp. 600–612, 2004.