Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

A Survey on Medical Image Security and Authentication Techniques

Ashish Sethi, Vishal Garg, Shiva Sharma, Manisha Rastogi*
Department of Biomedical Engineering
Shobhit Institute of Engineering and Technology
(A NAAC Acrediated Deemed to be University)
Modipuram, Meerut

Abstract: **- Communication technology has made it easier to access the medical services at distance locations, where doctors are not physically available. During transmitting the data between two servers, data can be changed or tampered with various attacks. Several stenography and watermarking techniques were used for the authentication and security of data. So the aim of this data to compare two techniques and to compare their efficiency. Results indicates that CDMA with DWT is comparatively better than the CDMA technique.**

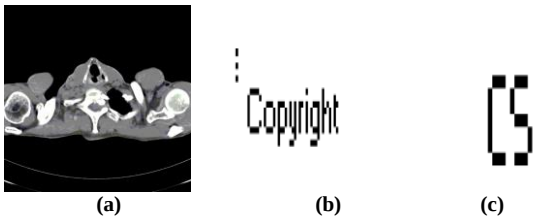
Keywords: Medical Images, CDMA Technique, CDMA with DWT, Image Quality Indices.

1. INTRODUCTION

With the development of the latest communication technology it has become very easy and usual to take the expert medical service, advise from all over the world. The accessibility to these medical services at host domain is the part of telemedicine. Telemedicine itself work for different medical related technology like teleradiology, telesurgery, telepathy, telecare, teledermatologist and teleneurology.[1] This technology involves the use of computer to receive, store and transmit the information to a distant location. Advancement in technology has reduces the difficulty to access the better healthcare, cost of the analysis, so working as a boon in medical sector. [2] To access this technology medical information is used to transfer or exchanged over the internet for several purposes as teleconference among clinicians, interdisciplinary exchange between clinicians and radiologists for consultative purposes or to discuss diagnostic and therapeutic measures and for distant learning of medical personnel. [3] Over the several benefits of these tele services there is a risk of security with medical data as Internet is the open network where anyone can access the database for illegal use also. [4] So there is a need of some authentication and protection technology to access the data and secure transfer of the data as security of medical information is the prime goal of the telemedicine services. There are several techniques like cryptography, Steganography and watermarking are available those are majorly used for the security and authentication of the data. But previous research work shows a viable limitation with the use of cryptography, Steganography and shown watermarking as the best technique. Digital watermaking shows its Robustness, Higher Embedding Capacity, provide communications one point-to-multiple points, these quality make it preferable for the medical information security. [5] It embeds copyright information in the original file and doesn't disturb the appearance of the original file. Not only is this it also difficult for the medical staff to maintain the patient record and information in form of file and the computers. So it can work as a secondary way where all the information and test reports would be embedded in the image itself. No other document is require to carry the with the patient. Whenever physician required can extract the information from the images itself. Watermarking itself broadly categories into spatial domain watermarking and frequency domain water technique. Here in this research work we are going to compare one spatial domain watermarking technique with Frequency domain watermarking technique. Aim of this research work is to check the efficiency of two different domain watermarking technique to investigate the strength and limitations of current watermarking scheme.

2. MATERIALS AND METHOD

A. Image: For this research work image was taken from TCIA dataset for medical images. It has majorly CT and MRI obtained Medical image. We have chosen CT cancer image. And the Watermark or Copyright image is formed in Bit Map Format image with 256 gray level, 8 bit depth, 512 X 512, 20 X 50 and 9 X 12. Watermark and Original images are used in same format and size for easy image processing. Matlab 12b is used as a working platform for this research paper.



(a) **(b)** **(c)**

Figure 1: (a) Original CT Cancer Image (b) Copyright Image (c) Copyright Image

B. Techniques: Here is this work the comparison would be carried out between two watermarking techniques in spatial and frequency domain, CDMA watermarking technique from Spatial and CDMA Watermarking with DWT will be use from frequency domain. The comparative analysis would be carried out by comparing Time required for embedding and recovery of the watermark, Signal to noise ratio, Robustness, Capacity, Tamper resistance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

C. CDMA watermarking: The proposed technique utilizes the concept of CDMA spread spectrum. According to which we scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping. A pseudo random noise (PN) pattern *W(x, y)* if added to cover image *I(x, y)*, to create a watermarked image according to the equation (1) as given below.

$$I_w(x,y) = I(x,y) + k * W(x,y) \quad (1)$$

k denotes a gain factor, and I_W the resulting watermarked image. Increasing *k* increases the robustness of the hidden message at the expense of the quality of the watermarked image. In case of recovery sequence matching procedure is repeated for all the values of the watermarked image. So, CDMA improves on the robustness of the hidden message significantly, but requires several orders more of calculation. [6]

Figure 2: (a) Embedding steps for watermark (b) Recovery steps for watermark in CDMA

D. CDMA watermarking with DWT: The main idea of embedding CDMA watermark is to embed randomly generated PN sequence into the horizontal, vertical or diagonal components of the DWT coefficients. The PN sequences are embedded into the horizontal and vertical component coefficients with certain gain k, when the watermark bit is zero, according to the following equation:

Hz= Hz + k * PN Sequence for horizontal components

Vz = Vz + k * PN Sequence for Vertical components

Where, Hz represents the coefficients of horizontal component and Vz represents coefficients of vertical component. The method used for recovery of the watermark is also very simple. The two PN sequences for horizontal and vertical component respectively are regenerated and their correlations with the horizontal and vertical component coefficients are found. If the average correlation crosses the threshold set at the mean correlation, the watermark bit is assumed to be 0 else 1. [7]

E. Performance Analysis Parameters

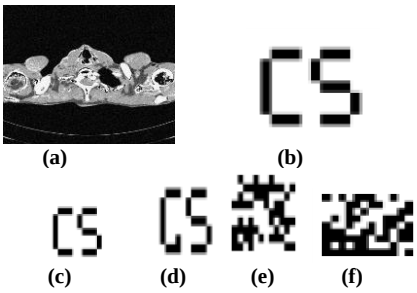
The performance analysis deals with various parameters to be calculated to check the robustness of the technique. The main goal of watermarking is to resist both geometric distortion and signal processing attacks. Since, no watermarking algorithm resists all the attacks. But, still one can find better technique which will give more robust watermark by performing various calculations. Aim of attack is to impair detection of watermark or destroy the embedded watermark. Attacks can be removal attacks, geometrical attacks, cryptographic attacks and protocol attacks. Robustness against attacks is an important aspect for watermarking schemes. [8-9]

Table 1: Performance Analysis Parameters

S.No.	Parameter	Indicator
1.	Accuracy	Accuracy is the nearness of a calculation to the true value. An accuracy of 100% means that the measured values are exactly the same as the given values.
2.	PSNR	The widely used peak signal-to-noise ratio (PSNR) measurement which measures the maximum signal to noise ratio found on an image is used as an objective measure for the distortions introduced by the watermarking system.
3.	Execution Time	Another important tool for evaluating algorithms is measurement of the amount of time required to embed a watermark into a host image, and then extract it afterwards. The actual time in CPU cycles will be used as a measure of execution time.
4.	MSE	MSE is mean square error between the original image Iorg and the watermarked one Iw.
5.	BCR	The use of the bit correct ratio (BCR) has become common recently, as it allows for a more detailed scale of values. The bit correct ratio (BCR) is defined as the ratio of correct extracted bits to the total number of embedded bits.
6.	Payload Capacity	Payload or capacity simply refers to the size of watermark that can be embedded in the cover image. The size is in terms of bits. Payload or capacity is another important characteristic because it has a direct negative impact on the robustness.
7.	SSIM	The structural similarity index measure the similarity between two images based on perceived change in image structure.
8.	Security	Security is related with the strength of embedded watermark protection in watermarked media. The security is assessed on the basis of length of time it takes to break the watermarking algorithm and reveal the hidden watermark.
9.	Normalized Cross Correlation	It is used to measure the similarity between the cover image and the watermarked image as well as original watermark and recovered watermark. Higher the value of NCC will result in better technique.
10.	Similarity Ratio	Similarity Ratio (SR) is the comparison between original watermark and extracted watermark.

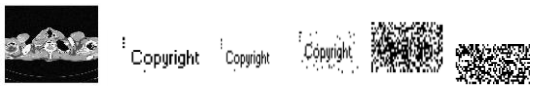
3. RESULTS

A. CDMA Spatial Domain:



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 07, July-2018

B. CDMA with watermarking



(a) (b) (c) (d) (e) (f)

Figure 3 (a) Cancerous Image watermarked using technique 1 and 2 (b) Retrieved watermark (c) Recovered watermark from watermarked image attacked by histogram equalization. (d) Recovered watermark from watermarked image attacked by Gaussian noise. (e) Recovered watermark from watermarked image attacked by median filter (3X3). (f) Recovered watermark from cropped watermarked image.

Table 2: Results Performance Analysis

S.No.	Parameter	CDMA Technique	CDMA with DWT
1.	Accuracy	80%	99.95%
2.	PSNR	6.8095e+004	166.5005
3.	Execution Time	2.297	2.995
4.	MSER	30.2991	30.5393
5.	BCR	95.5%	99.9%
6.	Payload Capacity	Less	High
7.	SSIM	0.8713	0.9832
8.	Normalized Cross Correlation	87.13	98.32
9.	Similarity Ratio	84.68%	95.36%

Table 3: Robustness analysis in the presence of various attacks

S.No.	Parameter	CDMA Technique	CDMA with DWT
1.	Noise Attack	70.3587	90.5129
2.	Blurring	60.3216	85.6737
3.	Rotation	68.4235	75.6401
4.	Permutation of Pixels	40.1783	70.3754
5.	Histogram equalization	71.2408	100
6.	Median filtering	50.6592	70.3704
7.	Gaussian noise	55.2734	99.0741
8.	Cropping	45.3704	77.7344
9.	Salt and Pepper Noise	72.1654	90.3745
10.	Speckle Noise	68.3675	89.62431
11.	Average Filter	71.6354	84.72641
12.	Rescaling	82.7654	97.4321
13.	Image Sharpening	94.1173	98.736
14.	JPEG	95.9102	100

4. CONCLUSION

On the basis of above parameters we can conclude that CDMA with DWT is better technique it has more transparency, imperceptibility and the robustness. Robustness in the technique with several attacks indicates it better performance. Payload capacity of this technique is also high so more data can be embedding comparatively CDMA only. This generates futuristic approach to in Medical Imaging domain and gives an insight to work in the same domain.

REFERENCES:

[1] P. Singh, R. S. Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”, International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 9, March 2013.

[2] C. Woo, "Digital Image Watermarking Methods for Copyright Protection and Authentication," Ph.D. Thesis, Queensland University of Technology, Australia, March 2007.

[3] N.A. Memon, S.A.M. Gilani, “Watermarking Of Chest Ct Scan Medical Images For Content Authentication,” *International Journal of Computer Mathematics*, vol. 20, pp. 753-762, Apr. 2010.

[4] G. Bleumer (2011) Encyclopedia of Cryptography and Security. [Online]. Available: http://www.informatik.unitrier.de/~ley/db/reference/crypt/crypt2011.html#Bleumer11p

[5] N. Singh, M. Jain, S. Sharma, “A Survey of Digital Watermarking Techniques”, International Journal of Modern Communication Technologies & Research (IJMCTR), Volume-1, Issue-6, 2013.

[6] T.Jayamalar and V. Radha, “Survey on Digital Video Watermarking Techniques and Attacks on Watermarks,” *International Journal of Engineering Science and Technology*, vol. 2, pp. 6963-6967, Jan. 2010.

[7] A.Tiwari1 and M. Sharma, “Comparative Evaluation of Semifragile Watermarking Algorithms for Image Authentication,” *Journal of Information Security*, vol. 3, pp. 189-195, Apr. 2012.

[8] N. Singh, S. Joshi, “Ambiguity Attacks on SVD Based Watermarking Technique. Proceedings of International Conference on Smart Trends for Information Technology and Computer Communications”, SmartCom 2016. Communications in Computer and Information Science, vol 628. Springer, Singapore (2016) August 6-7; Jaipur, India.

[9] N. Singh, S. Joshi, S. Birla, “False Watermark Extraction and Rewatermarking Issues with Image Watermarking Techniques”, *Indian Journal of Science and Technology* vol 10(7), pp: 1-6, 2017.