International Journal of Information Technology and Management

Vol. VIII, Issue No. XII, May-2015, ISSN 2249-4510

A STUDY ON THE VARIOUS TECHNIQUES USED IN WAVELET DOMAIN FOR INFORMATION SECURITY IN MEDICAL IMAGES

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VIII, Issue No. XII, May-2015, ISSN 2249-4510

A Study on the Various Techniques Used In Wavelet Domain for Information Security in Medical Images

Manish Mahajan

Research Scholar, Bundelkhand University, Jhansi, UP

Abstract – Modern healthcare systems are based on managing diagnostic information of patients in a digital way. To guarantee the security, authenticity and management of medical images and information through storage and distribution, the watermarking techniques are used. This research aims at developing a watermarking technique in wavelet domain which uses the Electronic Health Record (EHR) as watermark and hospital logo as the reference image.

----------X----------

INTRODUCTION

Embedding of the EHR data is based on energy band selection and in reference to the bit location in the reference image. Performance of the proposed method was tested for four modalities of medical images; MRA, MRI, Radiological, and CT. Simulation results show no visible difference between the watermarked and the original image.

Moreover, the proposed watermarking method is robust against a wide range of attacks such as JPEG compression, Gaussian noise addition, histogram equalization, contrast adjustment, sharpening and rotation.

Telemedicine combines Medical Information System with information technology that includes use of computers to receive, store and distribute medical information over long distances. Currently, telemedicine applications in tele-consulting, tele-diagnosis, tele-surgery and remote medical education play a vital role in the evolution of the healthcare domain.

The transmission, storage and sharing of electronic medical data via the networks have many purposes such as diagnosis, finding new drugs and for scientific research. Exchange of medical image between hospitals located in different geographical locations is a common practice.

Hence, healthcare industry demands secure, robust and more information hiding techniques promising strict secured authentication and communication through internet or mobile phones. In general information hiding includes digital watermarking and stegano-graphy.

A watermarking scheme imperceptibly alters a cover object to embed a message about the cover object (e.g owner's identifier). Watermarking is used for copyright protection, broadcast monitoring and transaction tracking and thus robustness of digital watermarking schemes becomes critical. In contrast, stegano-graphy is used for secret communications.

A Stegano-grahic method undetectably alters a cover object to conceal a secret message. Thus, steganographic methods can also hide the very presence of covert communications. In general, digital watermarking algorithms can be divided into two classes depending on the domain of watermark embedding. The first group belongs to the algorithms which uses spatial domain for data hiding ,while algorithms of the second group take advantage of transform domain like Discrete cosine Transform (DCT), Discrete Fourier Transform(DFT) and Discrete Wavelet Transform (DWT) for watermarking purpose.

Previous works reveals that transform domain schemes are typically more robust to noise, common image processing tasks and compression when compared with spatial transform schemes.

Digital watermarking can also be categorized into visible and invisible, fragile and robust, blind and non-blind with emphasis on authentication, rightful ownership, availability of the host image etc.

Researchers proposed watermarking techniques and reported findings in the literature survey both integrity and confidentiality requirements (Wang et al.,2000; Zhou et al,2001;Chao et al,2002;Giakoumaki et

al,2003;Shieh et al,2004; Piva et al,2005;Xuan et al,2006; Wang et al proposed to embed secret messages in the moderately significant bit of the cover image.

A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. They also proposed to use a local pixel adjustment process (LPAP) to improve the image quality of the stego image. As the local pixel adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution.

Zhou et al presented a method that attaches digital signature and EPR into the medical image. Their method uses LSB replacing technique to embed the signature.

Chao et al proposed a secure data hiding technique based on the bipolar multiple base conversion to allow a variety of EPR data to be hidden within the same mark image.

Giakoumaki et al presented a wavelet based multiple watermarking approach. Their method addresses confidentiality protection and data authentication problems by using three separate watermarks.

Shieh et al a genetic algorithm (GA) based watermarking scheme is presented.GA is used to locate the optimal frequency bands for watermark embedding.

Piva et al a simple and secure self-recovery authentication technique is presented which hides an image digest in sub-bands of Discrete Wavelet Transform.

Xuan et al have presented histogram shifting based reversible watermarking techniques. In this work, a part of the histogram of high frequency wavelet co-efficients shifted towards right by one point and then watermark is embedded by using the histogram zero point.

Based on good time frequency features and discrimination that match well with the Human Visual System (HVS) motivates the use of DWT in image watermarking among several techniques.

In medical applications, it is very important to maintain the quality of images because of their diagnostic value. The performance of watermarking schemes can be improved by several methods. Dual watermarking technique is one of the methods to increase the level of security on the watermarked data.

REVIEW OF RELATED LITERATURE

Ayman El-Baz et al. have employed a fully automatic Computer-Assisted Diagnosis (CAD) system for lung cancer screening using chest spiral CT scans. This paper presents a system for detection of abnormalities, identification or classification of these abnormalities with respect to specific diagnosis, and provides the visualization of the results over computer networks.

The process of detection of abnormalities, identification of these abnormalities can achieve by image analysis system for 3-D reconstruction of the lungs.

Riccardo Boscolo et al. proposed method that uses the novel segmentation technique that combines a knowledge based segmentation system with a sophisticated active contour model.

This method performs robust segmentation of various anatomic structures. In this approach the user, need to provide initial contour placement, and the required parameter optimization automatically determined by the high-level process.

Binsheng et al. reported the algorithm, which used the method of selecting the threshold value by analyzing the histogram. This algorithm initially separates the lung parenchyma from the other anatomical structures from the CT images by using threshold value.

By this algorithm structure in CT scan image with higher densities having some higher density nodules, can grouped into soft tissues and bones, leading to an incomplete extraction of lung mask. For having complete hollow free lung mask, morphological closing is applied in this approach.

Hossein B. et al. has introduced the model-based segmentation algorithm. In this approach instead of using model information to direct the segmentation algorithm for segmenting an organ of CT scan images, it uses this information to choose a segment with highest fidelity to the organ.

After completing with the segmentation of ROI, needs to proceed with medical image watermarking technique to provide security, authentication and privacy of this medical data.

There has been fair amount of work done in the area of medical image processing. Numbers of medical image watermarking schemes are reported in this literature survey, to address the issues of medical information security, and authentication.

Wakatani presented a medical image watermarking, in order not to compromise with the diagnosis value, it avoids embedding watermark in the ROI. In this algorithm watermark to be embed is firstly compressed by progressive coding algorithm such as Embedded Zero Tree Wavelet (EZW).

Embedding process is done by applying Discrete Wavelet Transform (DWT), for transforming the

original image using Haar basis. Extraction of watermark is reverse of embedding process. The major drawback of this algorithm is ease of introducing copy attack on the non-watermarked area.

Yusuk Lim et al. reported a web-based image authentication system, they used the CT scan images. This technique is mainly based on the principal of verifying the integrity and authenticity of medical images. In this approach, the watermark is preprocessed by using most significant bit-planes except least significant bit (LSB) plane of cover medical image, as a input to the hash function.

This hash function generates binary value of 0 or 1 using secrete key, which is then embedded in LSB bit of cover image to get watermarked image.

Rodriquez et al. proposed a method in which it searches a suitable pixel to embed information using the spiral scan that, starts from the centroid of cover image. Then by obtaining the block with its center at the position of selected pixel, it checks the value of bit to embed.

If bit value is 1, then the embedding information is obtained by changing the luminance value of the central pixel by adding the gray-scale level mean of the block with luminance of the block. In addition, if bit value is 0, then luminance value of the central pixel is changed by subtracting the luminance value of block from the gray-scale level mean of the block.

RESEARCH STUDY

Watermarking is an interdisciplinary study that draws experts from communications, cryptography and audio and image processing. Interesting new problems have been posed in each of these disciplines based on the unique requirements of watermarking applications.

Commercial implementations of watermarking must meet difficult and often conflicting economic and engineering constraints. Digital watermarking has been proposed as a new, alternative method to enforce the intellectual property rights and protect digital media from tampering.

It involves a process of embedding the digital signature into a host signal in order to "mark" the ownership. The digital signature is called the digital watermark. The digital watermark contains data that can be used in various applications, including digital rights management, broadcast monitoring and tamper proofing. The existence of the watermark is indicated when watermarked media is passed through an appropriate watermark detector.

A watermark, which usually consists of a binary data sequence, is inserted into the host signal in the watermark embedder. Thus, a watermark embedder has two inputs; one is the watermark message accompanied by a secret key and the other is the host signal (e.g. image, video clip, audio sequence etc.).

The output of the watermark embedder is the watermarked signal, which cannot be perceptually discriminated from the host signal. The watermarked signal is then usually recorded or broadcasted and later presented to the watermark detector.

The detector determines whether the watermark is present in the tested multimedia signal, and if so, will decode the message. The research area of watermarking is closely related to the fields of information hiding and steganography. The three fields have a considerable overlap and many common technical solutions.

However, there are some fundamental philosophical differences that influence the requirements and therefore the design of a particular technical solution. Information hiding (or data hiding) is a more general area, encompassing a wider range of problems than the watermarking. The term hiding refers to the process of making the information imperceptible or keeping the existence of the information secret.

The availability of different multimedia editing software and the ease with which multimedia signal are manipulated have opened many challenges and opportunities for the researchers. A possibility for unlimited copying without a loss of fidelity causes a considerable financial loss for copyright holders. The ease of content modification and a perfect reproduction in digital domain have promoted the protection of intellectual ownership and the prevention of the unauthorized tampering of multimedia data to become an important technological and research issue.

A wide use of multimedia data combined with a fast delivery of multimedia to users having different devices with a fixed quality of service is becoming a challenging and important topic. Traditional methods for copyright protection of multimedia data are not sufficient.

Hardware-based copy protection systems have already been easily circumvented for analogue media. Hacking of digital media systems is even easier due to the availability of general multimedia processing platforms, e.g. a personal computer. Simple protection mechanisms that were based on the information embedded into header bits of the digital file are not useful because header information can easily be removed by a simple change of data format, which does not affect the fidelity of media.

Encryption of digital multimedia prevents access of the multimedia content to an individual without a proper decryption key. Therefore, content providers get paid for the delivery of perceivable multimedia, and each client that has paid the royalties must be able to decrypt a received file properly.

Once the multimedia has been decrypted, it can be repeatedly copied and distributed without any obstacles. Modern software and broadband Internet provides the tools to perform it quickly and without much effort and deep technical knowledge.

It is clear that existing security protocols for electronic commerce serve to secure only the communication channel between the content provider and the user and are useless if commodity in transactions is digitally represented. From a business perspective, the question is whether watermarking can provide economic solutions to real problems.

Current business interest is focused on a number of applications that broadly fall into the categories of security and device control. From a security perspective, there has been criticism that many proposed watermark security solutions are “weak”, i.e. it is relatively straightforward to circumvent the security system. While this is true, there are many business applications where “weak” security is preferable to no security. Therefore it is expected that businesses will deploy a number of security applications based on watermarking.

In addition, many device control applications have no security requirement, since there is no motivation to remove the watermark. Device control, particularly as it pertains to the linking of traditional media to the Web, is receiving increased attention from businesses and this interest will increase. From an academic perspective, the question is whether watermarking introduces new and interesting problems for basic and applied research.

Compression is useful to lower consumption of expensive resources like hard disk space/transmission bandwidth (computing). But its disadvantage is that when compressed data is decompressed, it is detrimental for some applications.

For example, an image compression scheme may need a costly hardware for quick image decompression to be viewed as it is while under decompression (image decompressing before watching it could be inconvenient as image needs storage space). The design of data compression schemes thus involves trade-offs among various factors, including compression degree, amount of distortion introduced (when using a lossy compression scheme), and computational resources needed to compress and decompress data.

Image compression is a data compression application on digital images. Image compression minimizes a graphics file size in bytes without lowering image quality to unacceptable levels. File size reduction ensures adequate storage of additional images in given disk/memory space reducing time needed for image transmission over the net or for web pages downloading.

SIGNIFICANCE OF THE STUDY

A high priority ROI generated bit stream will appear early in the entire image bit stream. The background area with low priority will appear at the end stage of the whole image it streams. Image data separation: After ROIs selection, images are divided into ROIs and non-ROIs and the latter are processed by wavelet transform first as a coefficient matrix is needed as encoder input.

Image resolution enhancement focuses on modifying the resolution of an image so that the result is similar to the original image. Images can have geometric distortions due to different satellite view angles, variable ground resolution cell sizes, environmental conditions and directional reflectance effects from surface materials.

For overcoming these geometric distortions, satellite image resolution enhancement is very important in image processing applications. Here, a DWT based interpolation technique is proposed to improve the resolution of the satellite image.

The image classification technique is broadly divided into unsupervised and supervised learning techniques. Clustering algorithms used for unsupervised learning of remote sensing data vary according to the efficiency with which clustering takes place. The unsupervised clustering provides the cluster information about the water body in a relatively quick manner.

This lacks complete information about the region of interest and particularly subtle variations therein. To avoid unexpected groupings, supervised classification is recommended. The mapping of classes is much more accurate in supervised classification but is heavily dependent on the input given.

The classes of interest that are the water body and non-water body areas and the learning rate are determined to optimize the classification accuracy of the images.

This research aims to further improve the accuracy of classification by considering five texture features as input. A support vector machine is a supervised learning algorithm that analyze the inputs and recognize the water body and non-water body classes, used for classification and regression. The performance of the classification shows the

requirement of denoising and resolution enhancement technique.

REFERENCES

[1] L. P. Seidman., Sattelites for Telemedicine and Tele-health, Journal of telemedicine and telecare, vol 3 no. 1, pp. 101-102, 2007.

[2] R. Wootton, J. Blignault, J. Cignoli., A National Survey of Telehealth Activity in Australian Hospitals, Journal of Telemedicine and Telecare, vol 9 no. 2, pp. 73-75, 2003.

[3] S. Tachakra, X. H. Wang, R. S. Istepanian, Y. H. Song., Mobile e-health: The Unwired Evaluation of Telemedicine, Telemedicine Journal of e-health, vol 9 no. 3, pp. 247-257, 2002.

[4] D. Osborne, D. Rogers, J. Mazumdar, R. Coutts, D. Abbott., An Overview of Wavelets for Image Processing for Wireless Applications, Proceedings of SPIE: Smart Structures, Devices and Systems, University of Melbourne, Australia, vol 4935, pp. 427-435, 2002.

[5] Hussain N et. al., A review of medical image watermarking requirements for teleradiology. [Online], Journal of Digital imaging, 2012.

[6] Royal college of Radiologists, Standards and recommendation for the reporting and interpretation of image investigations by non-radiologist medically qualified practitioners and radiologist, 2011.

[7] Position Statement on International Teleradiology, the Royal Australian and New Zealand College of Radiologists, Version, Council, approval: March 2007.

[8] D. Maio, D. Maltoni, A.K. Jain, S. Prabhakar., Handbook of Fingerprint Recognition, Springer, Berlin, 2003.

[9] Jain A.K. et al., Filter bank-based fingerprint matching, IEEE Transaction on Image processing, vol. 9, no. 5, pp. 846-859, 2000.

[10] Ju Cheng Yang and Dong Sun Park., Fingerprint Verification Based on Invariant Moment Features and Nonlinear BPNN, International Journal of Control, Automation, and Systems, vol. 6, no. 6, pp. 800-808, 2008.