International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 4, No. 1
February 2015

National Conference on "Recent Trends in Communication & Information Technologies"NCRTCIT 2015

Organized by

Dept. of ECE, Indra Ganesan College of Engg., Trichy, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 1, March 2015
National Conference on "Recent Trends in Communication & Information Technologies" NCRTCIT 2015

Research Paper

FACE RECOGNITION USING THERMAL IMAGE WATERMARKING ALGORITHM FOR VERIFYING THE SECURITY ISSUES OF TELERADIOLOGY

R Pavithra[1]*, A Sabrina[1], E Velusamy and R Logarasu[1]

*Corresponding Author: ***R Pavithra***

Watermarking is the supreme chance from many reasearches around the world.It is the process of stagenography or embedding process.Digital watermarks can be used by a lot of applications like:copyright protection, data security, and data hiding and conveys other information etc.The Watermarking project security is improved by facial signature authentication using thermal image technique.A new thermal imaging framework with unique features extraction and similarity measurements for face recognition is presented.Teleradiology desires confidentiality, availability, and reliability which means only an authorized user can right to use patient data, guarantee access to medical information in normal scheduled conditions, prove that information has not been changed by unauthorized persons, and information beginning of its attachment relay to one patient.To offer all these aspects, teleradiology requires watermarking for well-organized maintenance and transmission of medical data remotely.The benefit of this technique is as long as security, avoid host interferences and get better the decoder performance.Embedding data to the video frames is achieved by following steps. At first step, by using string technique data is watermarked to an image. At second step, data embedded image is watermarked to a selective frames in the video sequence by using watermarking technique.Watermarking object is retrieved by using technique without any data loss.

Keywords: Digital watermarking, Facial signature authentication, Teleradiology, DWT

INTRODUCTION

Digital Watermarking

The term watermark was introduced near the end of the 18th century.During the past decade, with the development of information, digitalization and internet; digital media increasingly predominate over traditional analog media. However, as one of the concomitant side-effects, it is also becoming easier for some individual or group to copy and transmit digital products without the permission of the owner. The digital watermark is then introduced to solve this problem. Covering many subjects such as signal processing, communication theory and Encryption, the

[1] Department of ECE, Selvam College of Technonolgy, Namakkal-637003.

research in digital watermark is to provide copyright protection to digital products, and to prevent and track illegal copying and transmission of them. Watermarking is embedding information, which is able to show the ownership or track copyright intrusion, into the digital image, video or audio. Its purpose determines that the watermark should be invisible and robust to common processing and attack.

Digital watermarking is the process of embedding Information into a digital signal which may be used to verify Its authenticity or the identity of its owners, in the same Manner as paper bearing a watermark .For visible Identification. In digital watermarking, the signal may be Audio, pictures, or video. If the signal is copied, then the Information also is carried in the copy. A signal may carry several different watermarks at the same time (Shraddha S Katariya (Patni), 2012).

In Embedding stage, the image to be watermarked is preprocessed to prime it for embedding. This involves Converting the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier Transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bit stream or a Pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired Coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse Transform on the altered transform coefficients (Peter Meerwald and Andreas Uhl, 2001).

Classification of Digital Watermarking

1) Digital watermarking can be divided into robust watermarking and fragile watermarking according to its Characteristics.Robust watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, the watermark is not destroyed after some attack and can still be detected to provide certification. Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

2) Digital watermarking can be divided into visible watermarks and invisible watermark.visible watermarks: A visible alteration of the digital image by appending a “stamp” on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity.Invisible watermarks: By contrast, an invisible watermark, as the name suggests that this is invisible for the most part and is used with a different motive. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and non-repudiation

Priciple of Digital Watermarking

Digital watermarking is the process of embedding information in to a digital signal in a way that is difficult to remove.the signal may be audio, pictures oe video,for example if the sigmal is

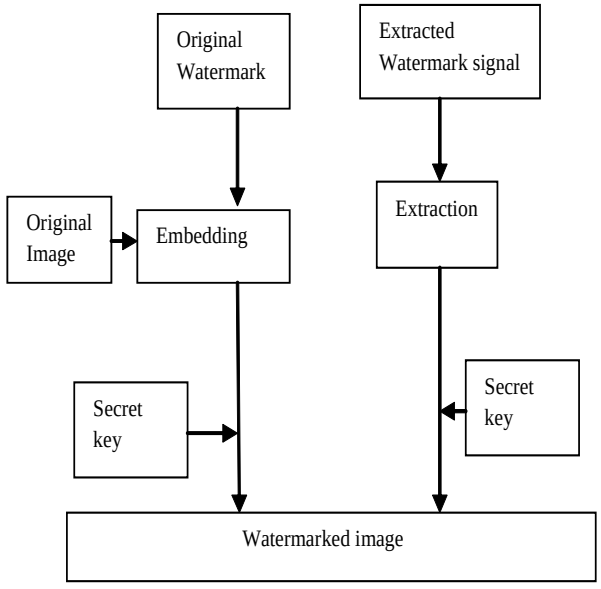
copied,then the information is also carried the copy. A signal may carry several different watermarks at the same time.

Common watermarking algorithms usually include two steps: watermark embedding And watermark detection.

Embedding the Watermark signal into the Host signal:

1. Host signal is selected.
2. A watermark signal is selected.
3. The least significant bits (LSBs) of the host signal will be replaced by the most significant bits (MSBs) of the watermark signal.
4. A watermarked signal is obtained which contains the host signal with its LSBs replaced by the MSBs of watermark signal.

Figure 1: Principle of digital watermarking



Compression of the watermarked signal:

1. Watermarked image watermarked is read
2. Discrete Cosine Transform is applied
3. Block is compressed through quantization or Huffman coding

Decompression of the watermarked signal:

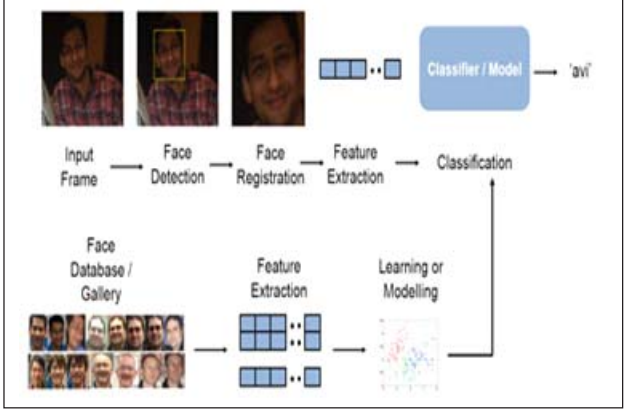
The compressed signal will now be decompressed

Removing the watermark from the watermarked signal:

1. The watermark from the watermarked signal is removed
2. It gives host signal and the watermark signal
3. Facial Recognition With Digital Watermarking

Biometric identifiers rely on fingerprint, iris, voice, gait and etc. It is rather easy for an individual to falsify attribute and biographical identifiers; however, biometric identifiers depend on intrinsic physiological characteristics that are difficult to falsify or alter. Applications for face recognition can be found in the areas of entertainment, smart cards, information security, law enforcement, medicine, and security. Diverse techniques and systems have been created for face detection in areas that use cameras in the visible spectrum. Facerecognition concept is the one of the successful and important application of image

Figure 2: Face recognition



anlysis.It is the process of identifying an individual using their facial features and expressions which individuals typically remember greater and for longer periods of time other their other qualities such as name.it is the one of the identification method.the ability of a computer to scan, store and recognize human faces for use in identifying people.The example of face recognition is given below.

Digital watermarking of face recognition usig thermal images has been explored to solve the problems of security of data. Biometric data security concerns are receiving the widespread public acceptance of biometric technology. Since a number of securities mechanism have been proposed, but due the trade-off between identification efficiency and security of stored template, practical applications have not benefited up to desired level. In this paper, we have designed a watermarking algorithm to improve the recognition performance as well as the security of a face recognition usig thermal images based biometric system.

The proposed algorithm provides the effective solution of security issues regarding biometrics techniques without affecting the face recognition usins thermal image quality. This algorithm is used in this step to segment the face of the subject from the rest of the image. The algorithm operates by first dilating the user-selected initial contour to create a potential localized region R for finding the optimal segmentation. Thus

$$R = \Phi \text{ (XOR) } S$$

where S is a spherical structuring element of the localization radius (i.e., 5 pixels) and (XOR) is the dilation operator.

Face recognition is significance identification method among the various identification techniques and we are working on it in order to increase the degree of security with the help of watermarking technique.Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering the file itself. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic. Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership (Cox I J *et al*., 1997). Various digital watermarking techniques are purposed for copyright protection of multimedia data from being misused (Swanson M D *et al*., 1998; Low S H *et al*., 1998) Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer (Md. Mahfuzur Rahman and Koichi Harada, 2006),. Watermarking algorithms are divided into two categories. Spatial-domain techniques work with the pixel values directly. Frequency-domain techniques employ various transforms, either local or global. Several widely recognized techniques are described subsequently (Hamad Hassan M and Gilani A A M, 2005).

Watermarking System

Multiplicative Spread Spectrum was used for data hiding but the interference result of the host signal leads to the decoding recital degradation to conquer this result An Improved Multiplicative Spread Spectrum scheme (IMSS) was developed. In IMSS scheme the host signal and the watermarked signal are compared at the decoder due to that the host interference is removed and it also works efficiently with the presence of additional Gaussian noise. DCT

algorithm was used to analyze the Bit error rate (BER), Peak signal to noise ratio (PSNR) and decoding performances of the MSS and IMSS.

Watermarking algorithm can be divided into spatial domain algorithm and transform domain algorithm. Spatial domain algorithms: Spatial domain digital watermarking algorithms directly load the raw data into the original image. It includes Last significant bit algorithm, Patchwork algorithm,Texture mapping coding method. Transform domain algorithm is a method of hiding data similar to spread-spectrum communication technology.Firstly, it does a kind of orthogonal transformation for image,and then embed watermark information in the transform domain of image, finally use the inverse transform to recovery the image in spatial domain, the detection an extraction of the watermark are also realized in transform domain. There are several common used transform domain methods, such as discrete Fourier transform (DFT), discrete cosine transforms (DCT), and discrete wavelet transforms (DWT), and so on.

DCT based watermarking techniques are more robust as compared to spatial domain watermarking techniques. this algorithm is robust against simple image processing operations like low pass filtering, contrast and brightness adjustment, etc. However, they are difficult to implement and are computationally more costly. And also they are weak against geometric attacks like scaling, rotation and cropping etc. DCT watermarking can be classified into Block based DCT watermarking and Global DCT watermarking One of the first algorithms presented by Cox et al. (1997) used global DCT to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS). Embed the watermark in the perceptually significant portion of the image has many advantage because most compression algorithms remove the perceptually insignificant portion of the image. It represents the LSB in spatial domain however it represents the high frequency components (Guan-Ming Su, 2001) in the frequency domain.

PROPOSED SYSTEM

Watermarking is the process of stagenography or embedding process. It is mainly proposed for copyright protection, data security, and data hiding and conveys other information etc. The Watermarking project is achieved by spread spectrum technique. Teleradiology needs confidentiality, availability, and reliability which means only an authorized user can access patient data, guarantee access to medical information in normal scheduled conditions, prove that information has not been altered by unauthorized persons, and information origins of its attachment relate to one patient. To provide all these aspects, teleradiology requires watermarking for efficient maintenance and transmission of medical data remotely. The advantage of this technique is providing security, avoid host interferences and improve the decoder performance. Embedding data to the video frames is achieved by following steps. At first step, by using string technique data is watermarked to an image. At second step, data embedded image is watermarked to a selective frames in the video sequence by using spread spectrum watermarking technique. Watermarking object is retrieved by using technique without any data loss. DWT domain provides decomposition in an object.

DWT DOMAIN WATERMARKING

In the last few years wavelet transform has been widely used in signal processing in watermarking,

general and image compression schemes. In some applications wavelet based watermarking schemes better than DCT based approaches.

A. Characteristics of DWT

1) The wavelet transform decomposes the image into three spatial directions, i.e. vertical, horizontal and diagonal. Hence Wavelets reflect the anisotropic properties of HVS more precisely.

2) Wavelet Transform is mathematically efficient and can be implemented by using filter convolution simply.

3) Magnitude of DWT coefficients is high in the lowest bands (LL) at each level of decomposition and is least for other Bands (HH, LH, HL).

4) The high magnitude of the wavelet coefficient the more significant.

5) Detecting watermark at lower resolutions level is effective because at every resolution level there is little frequency Bands present.

6) High resolution sub bands helps to easily positioned edge and patterns of textures in an image.

B. Advantages of DWT over DCT

1) Wavelet transform in HVS more closely than the DCT.

2) Wavelet transformed image is a multi-resolution description of image. Hence an image is shown at different resolution Levels and can be continuously processed from low resolution to high resolution.

3) Visual artifacts introduced by wavelet transformed images are less marked compared to DCT because wavelet

Transform doesn't decompose the image into blocks for processing. At high compression ratios blocking artifacts are Noticeable in DCT; but in wavelet coded images it is much clearer.

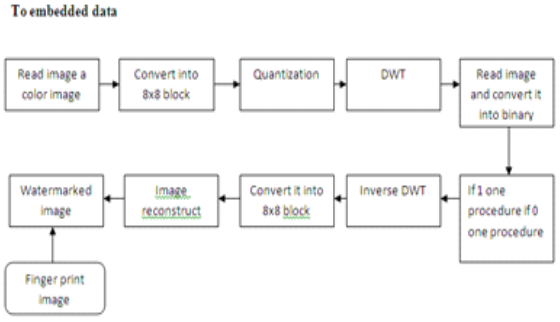
4) DFT and DCT are full frame transform, and hence any change in the transform coefficients affects the entire image

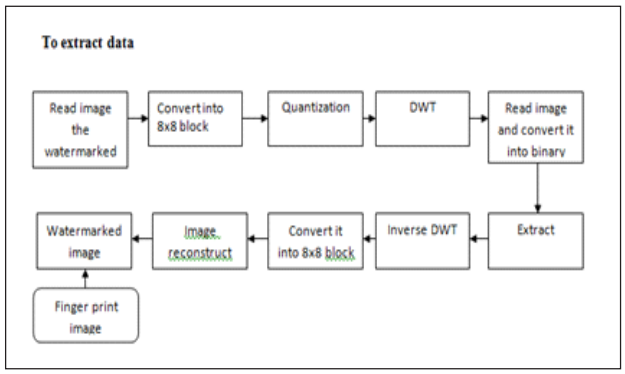
Except if DCT is implemented using a block based approach. However DWT has spatial locality property, which means if signal or any watermark is embedded it will affect the image locally. Hence a wavelet transform provides both frequency and spatial information for an image.

C. DWT watermarking

DWT based watermarking schemes use the same guidelines as DCT based schemes, i.e., concept is the same; however, Transformation process of an image into its transform domain varies and hence the resulting coefficients are different. Wavelet transforms use different kind of filters to transform the image. There are many filters, but the most commonly Used filters for watermarking are Haar Wavelet Filter, Daubechies Bi-Orthogonal Filters and Daubechies Orthogonal Filters. Each of these filters decomposes the image into many frequencies. Single level decomposition gives four Frequency sub band of the images. These

Figure 3: Block diagram of watermark embedding using DWT





four representations are called the LL, LH, HL, HH sub bands. In this part, we discuss wavelet based watermarking algorithms. We classify these algorithms based on their Decoder requirements as Non-blind Detection or Blind Detection. In, blind detection, original image for detecting the Watermarks don't require; but, non-blind detection requires the original image.

The Watermark embedding process consists of the following steps:

1. The original image is first resized into 512x512 pixels because after DWT decomposition, we will get only with 256x256 pixel size image.
2. As, the size of our watermark is 32x32, 256x256 is the exact dimension to embedded 32x32 pixels on 8x8 sub-blocks in complete image.
3. Then this is decomposed through 1-level Discrete Wavelet Transform which leads the image into four parts as explained above.
4. After this, watermark is embedded into the Low-high frequency components.
5. Then again, 1-level IDWT is applied to this image to synthesize it to complete image.
6. The final image is watermarked image.

The watermark extraction process

1. The watermarked image is resized into 512x512 pixels if needed.
2. The watermarked image is decomposed into 1-level DWT transform.
3. Then according to the embedding process, the comparison is done for extraction.
4. The generated image by comparison is the extracted watermark image.

RESULTS AND DISCUSSION

In this experiment 512x512 images are used to hide the data sequence. We can embedded 1024 bit in to the image more number of data's also possible because of time compaction minimum amount of bits only considered if the number of data increase, size of the image must be increased Watermarking depends upon the size of the image. Spread spectrum technique is used for watermarking.In previous work they are achieved average PSNR value of 37 db.in proposed method the PSNR value is raised compare to previous work .

Figure 4: Simulation Result DWT

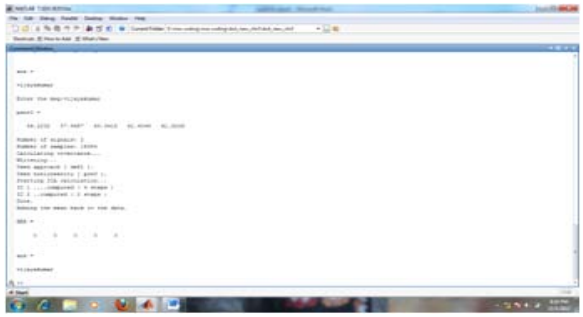


Figure 5: BER of DWT

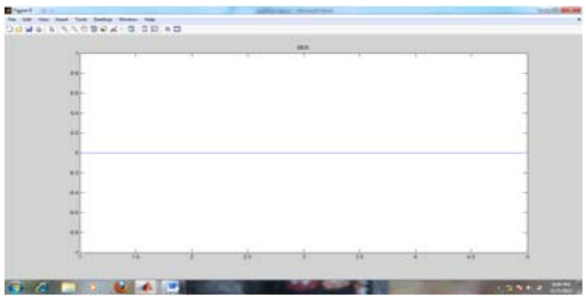


Figure 6: PSNR of DWT

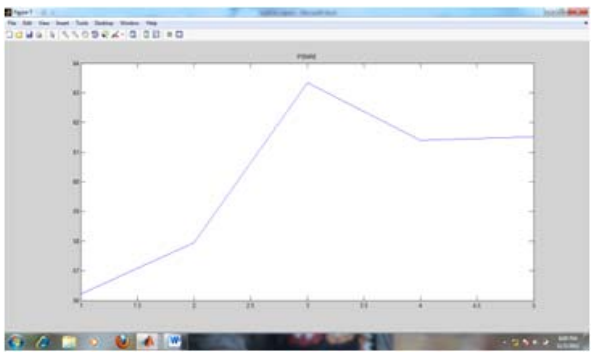
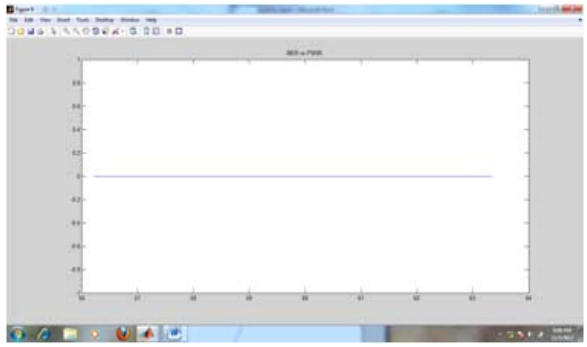


Figure 7: BER vs PSNR of DWT



As in the comparison with DCT algorithm DWT has that its more performance and scalability provided with its peculiar feature of executing at minimum time. And it provides increasing PSNR, better BER performance and improves the decoder performance and provides high security.

CONCLUSION

This paper has been presented biometric facial recognition using thermal image watermarking algorithm,embedding methods and extraction process. Also a basic techniques for the watermark process was presented.The proposed watermarking algorithms have been presented,which show advantages in systems using wavelet transforms with SVD.Another highlight is the replacement of DWT instead of DCT which improves computational performance and has an easier hardware implementation.In future works, the use of coding and cryptography watermarks will be approached.

REFERENCES

1. Cox I J, Kilian J, Leighton T and Shamoon T (1997), "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transaction on Image Processing*, Vol. 6, No. 12, pp. 1673-1687.
2. Guan-Ming Su (2001), "An Overview of Transparent and Robust Digital Image Watermarking".
3. Hamad Hassan M and Gilani A A M (2005), "A Fragile Watermarking Scheme for Color Image Authentication", *International Journal of Applied Science, Engineering and Technology*, Vol. 1, No. 3, pp. 156-160.
4. Low S H, Maxemchuk N F and Lapone A M (1998), "Document identification for copyright protection using centroid detection", *IEEE Trans. Commun.*, Vol.46, pp. 372-383, March.
5. Md. Mahfuzur Rahman and Koichi Harada (2006), "Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data", *IJCHNS International Journal of Computer Science and Network Security*, Vol. 6, No. 2A.
6. Peter Meerwald and Andreas Uhl (2001), "Digital Watermarking in the Wavelet Transform Domain", January.
7. Shraddha S Katariya (Patni) (2012), "Digital Watermarking: Review", *International*

Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, No. 2.

8. Swanson M D, Kobayashi M and Tewfik A H (1998), "Multimedia data embedding and watermarking technologies", *Proc. IEEE*, Vol. 86, pp.1064-1087, June.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com