ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

A Fingerprint Watermarking Algorithm for Verifying the Security Issues of Teleradiology

D.Praba[1], N.Padmapriya[2]

PG Student, Selvam College of Technology, Namakkal, Tamilnadu, India[1]

Assistant Professor, Selvam College of Technology, Namakkal, Tamilnadu, India[2]

ABSTRACT: 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 security is improved by fingerprint 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 watermarking technique. Watermarking object is retrieved by using technique without any data loss. DWT domain provides decomposition in an object.

KEYWORDS: Watermarking, Fingerprint, Dwt

I.INTRODUCTION

1.1 DIGITAL WATERMARKING

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 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.

Watermarking is the process of stereography 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.

Currently the digital watermarking technologies can be divided into two categories by the embedding positionspatial domain and transform domain watermark. Spatial domain techniques developed earlier and is easier to implement, but is limited in robustness, while transform domain techniques, which embed watermark in the host's transform domain, is more sophisticated and robust. With the development of digital watermarking, spatial techniques, due to their weakness in robustness, are generally abandoned, and frequency algorithm based on DCT or DWT becomes the research focus. Another tendency in watermarking is blind extraction, which means the host is not need when extracting the watermark; otherwise it is hard to avoid the multiple claims of ownerships.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

1.2 THE FOUNDATION OF DIGITAL WATERMARKING

It should be noted that the reason why digital watermarking is possible is that human vision system (HVS) is not perfect. Digital watermark utilizes the limitation of HVS to make it invisible, thus avoiding degrading original digital products, as well being hard to get identified or destroyed.

1.3 PROPERTIES AND REQUIREMENTS OF DIGITAL WATERMARKING

1.3.1 Invisible

A watermarking system is of no use if it distorts the cover image to the point of being useless, or even highly distracting. Ideally the watermarked imaged should look indistinguishable from the original even on the highest quality equipment.

1.3.2 Robust

The watermark should be resistant to distortion introduced during either normal use (unintentional attack), or a deliberate attempt to disable or remove the watermark present (intentional, or malicious attack). Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing, contrast enhancement…etc.

1.3.3 Unambiguous

Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

1.4 CLASSIFICATION OF DIGITAL WATERMARKING

1.4.1 Domain for watermark embedding

Spatial-domain watermarking technologies change the intensity of original image or gray levels of its pixels. This kind of watermarking is simple and with low computing complexity, because no frequency transform is needed.

However, there must be tradeoffs between invisibility and robustness, and it is hard to resist common image processing and noise. Frequency-domain watermarking embeds the watermark into the transformed image. It is complicated but has the merits which the former approach lacks.

1.4.2 Watermark detection and extractions

Blind-extracting watermarking means watermark detection and extraction do not depend on the availability of original image. The drawback is when the watermarked image is seriously destroyed; watermark detection will become very difficult. Nonblind-extracting watermark can only be detected by those who have a copy of original image. It guarantees better robustness but may lead to multiple claims of ownerships.

1.4.3 Ability of watermark to resist attack

Fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from heavily attacked watermarked image. Thus it is preferred in copyright protection.

1.5 THE PROCESS OF DIGITAL WATERMARKING

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

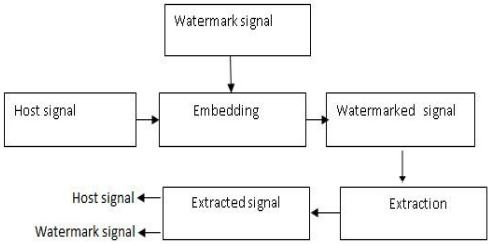


Figure 1.1 Block diagram of general watermarking

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

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

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

1.9 FINGER PRINT WITH DIGITAL WATER MARKING

Digital watermarking of fingerprint 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 security 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 fingerprint based biometric system.

- The proposed algorithm provides the effective solution of security issues regarding biometrics techniques without affecting the fingerprint quality. We have used fingerprint Verification Competition 2004 (FVC 2004) as a database for implementation of proposed algorithm. Experimental results show the efficacy of our algorithm.

- In recent years, the digital transmission of biometric data has introduced flexible, cost effective communication models that are beneficial in various transactions. At the same time, they also possess some serious drawbacks that digital data can be duplicated very easily without introducing any quality degradations to the content. Digital watermarking is a technique that is used to solve this problem. This does not allow an individual, other than the owner, to manipulate, duplicate, or access media information without owner's permission.
- This inspires a lot of research efforts in digital watermarking of biometrics. Fingerprint 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. Andrew Tirkel and Charles Osbome introduced "digital watermark" term in 1992. "Digital watermarking" is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents without affecting the overall quality of the original content. Digital watermarks are electronic way to embed the information on any multimedia content. Digital watermarks are used to uniquely identify the image in order to claim for the original content/image. These watermarks may be in form of text or image.
- In this paper we have used text watermark and embed on fingerprint images to make an appropriate belongingness or authentication. Thus, it is used to provide the security of contents in form of data protection. Watermarking techniques can be classified into different categories. Broadly these techniques can be classified into four areas according to the type of place to be watermarked as follows. Watermarking on images is called as image watermarking, if one apply watermark on videos referred as video watermarking, watermarking of audio signal come under the heading of audio watermarking and if watermarking has been applied on text this is called as text watermarking.
- If we want to classify according to the human perception, the digital watermarks can be divided into three different types as follows. Visible watermark: - The information is visible in the picture or video. Typically, the information is text or logo, which identifies the owner of the media. Invisible- Robust watermark: - if the watermarked content is equivalent to the original, un-watermarked content it is easy to create robust watermarks or imperceptible watermarks, but the creation of robust and imperceptible watermarks has proven to be quite challenging.
- Invisible-Fragile watermark: - it is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. From application point of view digital watermark can be classify as Source based or Destination based. Source based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. Destination based watermark can be used to trace the buyer in the case of illegal reselling.

II. WATERMARKING SYSTEM

Multiplicative Spread Spectrum was used for data hiding but the interference effect of the host signal leads to the decoding performance degradation to overcome this effect 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.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

2.1 Watermarking based on DCT

The DCT transform a signal from a spatial representation into a frequency representation. Lower frequencies are more obvious in an image than higher frequencies so if we transform an image into its frequency components and throw away a lot of higher frequency coefficients, we can reduce the amount of data needed to describe the image without sacrificing too much image quality. The discrete cosine transform (DCT) represent an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that, for a typical image most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. In this algorithm, the original image is divided into several 8x8 blocks. Then those several blocks are discrete cosine transformed (DCT-2). The watermark is embedded by 8*8 piecemeal and then again passed through Inverse DCT-2. The watermarking scheme consist of DCT transform of original image which will concentrate the main image information into the least low frequency coefficients, and cause smallest image blocking effect, thus achieves good compromise between centralized information and computational complexity. Moreover, 2D-DCT is real transformation. It has good energy compression ability, goes to the related ability envelope compatibility with the international compression standard. It is a good choice about using the 2D-DCT transform to implement the watermarking embedding and extraction. Figure 3.1 and 3.2 shows

The watermark Extraction process consists of following steps:

1. Firstly the watermarked image is resized into256x256 pixels if needed.
2. Then watermarked image is again block processed into 8x8 pixels.
3. Then Forward 2D-DCT is applied on the block processed image to have frequency separation.
4. After this, Extraction process is done in the same way as embedding was done in embedding process.
5. Depending upon the comparison done with particular pixels on which watermark datawas embedded, decision is make which is stored in again 32x32 empty array.
6. Then this matrix is the extracted image which was original watermark image.The embedding and extraction procedure of watermark.

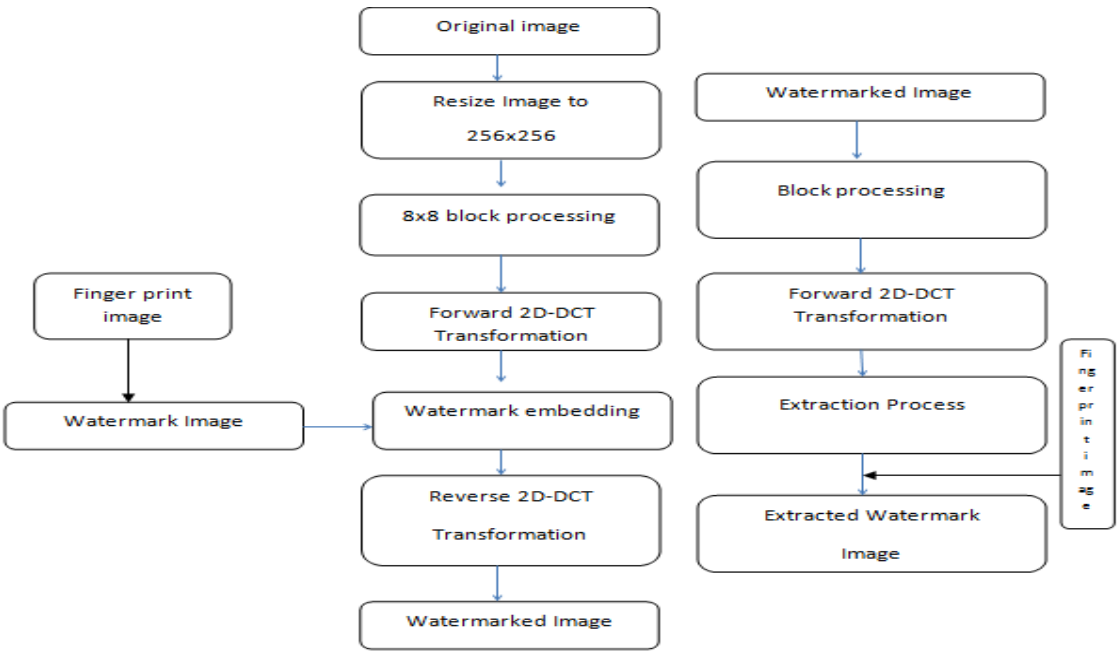


Figure2.1 DCT Watermark embedding

The watermark Embedding processes consists of following steps:

1. The original image is first resized into 256x256 pixels.
2. The watermark is resized into 32x32 pixels.
3. Then original resized image is block processed into 8x8 blocks so as to completely embed the 32x32 watermark on 256x256 images.
4. After this, 2D- Discrete Cosine Transform is applied on these 8x8 sub-blocks individually to convert it from time domain to frequency domain.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

5. The watermark image is embedded on the 8x8 blocks in the middle frequency band.
6. For embedding watermark, the value of frequency coefficient is changed in accordance to watermark data.
7. Reversed 2D-DCT is performed afterward on the watermark embedded image to convert from frequency domain to time domain.
8. The final image is the watermarked image

III. 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.

3.1 Watermarking Based On DWT

In this algorithm, the original image is first resized to 512x512. Then this is decomposed through 1- level Discrete Wavelet transform. Discrete wavelets transform is frequency domain analysis method which can localize frequency domain.

To embedded data

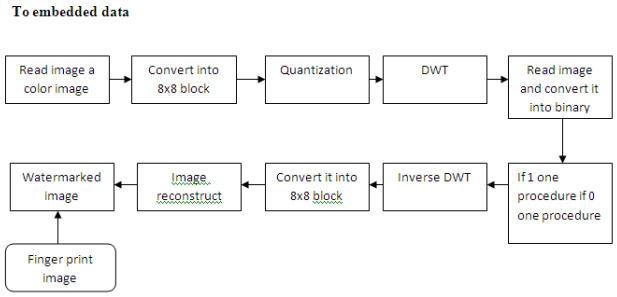


Figure: 3.1 Block diagram of watermark embedding using DWT

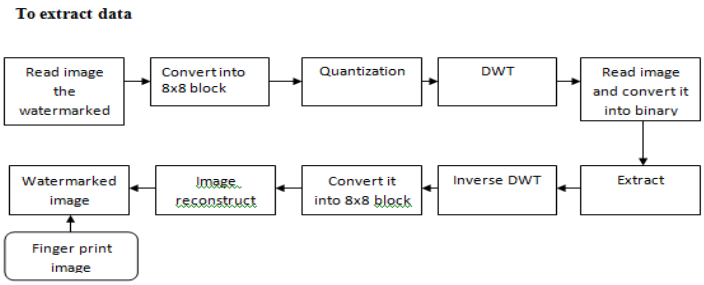


Figure: 3.2 Block diagram of watermark extraction using DWT

The basic idea of discrete wavelet transform (DWT) in image processing is to multi-differentiated decompose the image into 4 frequency districts which is one low frequency district(LL) and three high frequency districts (LH,HL,HH). L and H represent Low-pass and High-pass filter. 2-level DWT decomposition. The information of low frequency district image is very close to the original image. The frequency district of LH, HL, and HH respectively represents the level detail, the upright detail and the diagonal detail.

The human eye is sensitive to the change of smooth district of image, but not at the edges and peaks. So, it is not safe to putting watermark in coefficients of high frequency band of DWT image because it can be easily noticed. The brightness masking on human visual model shows that the larger the background brightness, the more the just noticeable difference of embeddable signal,

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

which means low frequency approximate image can be embedded by more watermarking capacity is lower than JND, as human eyes cannot suspect the existence of signal. Some common attacking to low frequency coefficients, the host image is also destroyed. So it is good to embed watermark in medium and low frequency. The figure 3.3 and 3.4 shows the watermarking based on DWT

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.

3.2 Advantages of proposed system

An advantage of the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, and HH) Embedding.

Sometimes your image may not be displayed in gray scale even though you might have converted it into a gray scale image. You can then use the command colormap(gray) to "force" Matlab to use a gray scale when displaying an image. If you are using Matlab with an Image processing tool box installed, I recommend you to use the command imshow to display an image.

3.3 KEY FEATURES

1. Spatial transformations and image registration
2. Image transforms, including FFT, DCT, Radon, and fan-beam projection
3. Workflows for processing, displaying, and navigating arbitrarily largeimages
4. Modular interactive tools, including ROI selections, histograms, and distance measurements
5. ICC color management
6. Multidimensional image processing
7. Image-sequence and video display

1. RESULT AND DISCUSSION

a. Experimental result

2. 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. DWT algorithms are used to embedand decode the data in to image, and analysis the BER and PSNR and plot the graph for respected values. The following table is used to represent the corresponding PSNR and BER for various images.
3. .

4. IMAGE	5. PSNR	6. BER
7. Lena gray	8. 61.4048	9. 0
10. Lena color	11. 61.4048	12. 0
13. Baboon gray	14. 56.2232	15. 0
16. Camera gray	17. 57.9487	18. 0
19. Girl face gray	20. 63.3415	21. 0
22. Average	23. 60.5	24. 0

Table 6.1 Average PSNR and BER

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

In previous work they are achieved average PSNR value of 37 db.in proposed method the PSNR value is raised compare to previous work is shown in the above table

a. SCREEN SHOTS

a. Figure 6.1 – 6.6 shows the output of proposed work

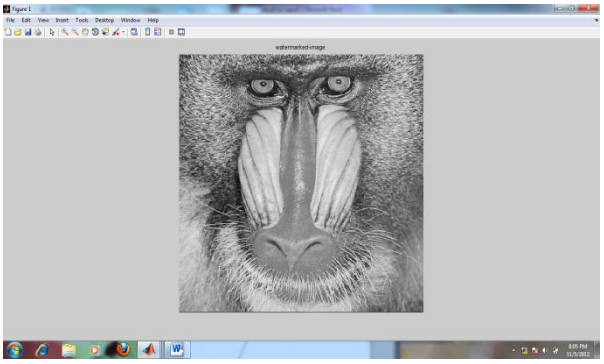


Figure 4.1 Baboon gray image

Figure 4.2 Camera gray image

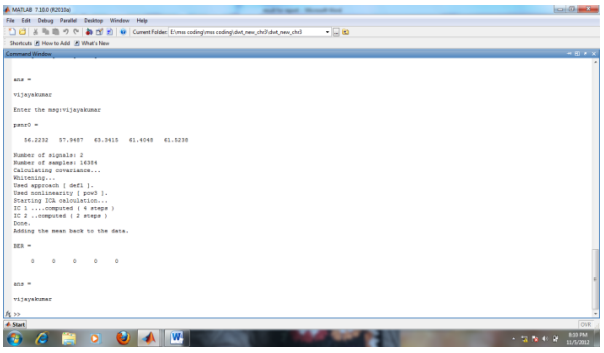


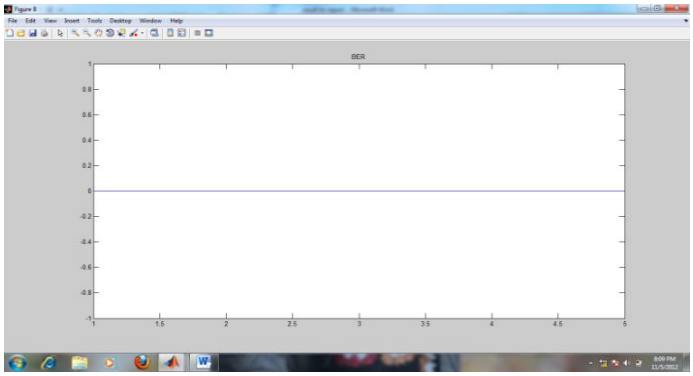
Figure:4.3 Simulation Result DWT

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015



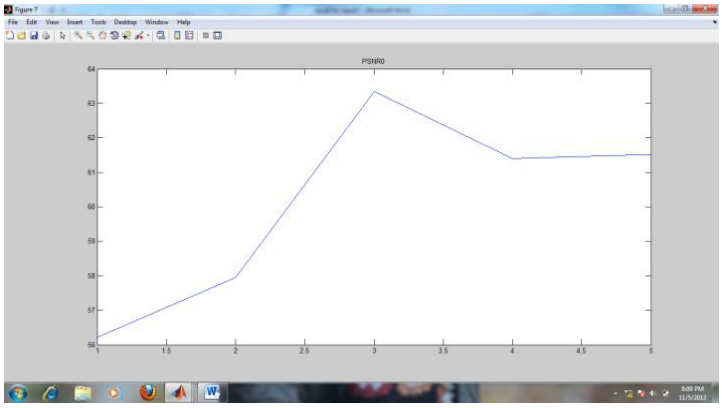


Figure:4.5 PSNR of DWT7

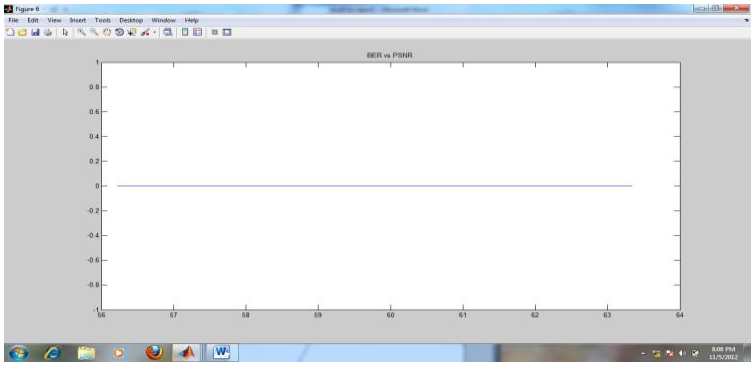


Figure:4.6 BER vs PSNR of DWT

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.

REFERENCES

1. Amir Valizadeh, and Z. Jane Wang,An "Improved Multiplicative Spread Spectrum Embedding Scheme for Data Hiding" IEEE transactions on information forensics and security, vol. 7, no. 4, august 2012.

2. NimaKhademiKalantari and Seyed Mohammad Ahadi "A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding" IEEE transactions on image processing, vol. 19, no. 6, june 2010.

3. Fernando Pérez-González, Carlos Mosquera, Mauro Barni, and Andrea Abrardo "Rational Dither Modulation: A High-Rate Data-Hiding

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Method Invariant to Gain Attacks "IEEE transactions on signal processing, vol. 53, no. 10, october 2005.

4. Ingemar J. Cox Joe Kilian, F. Thomson Leighton, and TalalShamoon, "Secure Spread Spectrum Watermarking for Multimedia" IEEE transactions on image processing, vol. 6, no. 12, december 1997.
5. Qiang Cheng "Generalized Embedding of Multiplicative Watermarks" IEEE transactions on circuits and systems for video technology, vol. 19, no. 7, july 2009.
6. Henrique S. Malvar, and Dinei A. F. Florêncio, "Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking" IEEE transactions on signal processing, vol. 51, no. 4, april 2003.
7. Jidongzhong and shangtenghuang "An enhanced multiplicative spread spectrum watermarking scheme" IEEE transations on circuits and systems for viedo technology, vol 16, no.12, december 2006.