
AN IMPLEMENTATION OF ENTROPY BASED DIGITAL WATERMARKING USING 2-D BIORTHOGONAL WAVELETS

Ajay Rattan

Ph.D Scholar

Computer Engineering

NIILM University

Kaithal, Haryana

Dr. Pankaj Kumar Verma

Associate Professor

Department of CSE

NIILM University

Kaithal, Haryana

ABSTRACT: With the widen use of internet, digital media are widely used. Digital media are easily and illegally destroyed, copied and change. So there is a need of transmitting the data securely and confidentially and for this we need an effective data hiding scheme. This is where watermarking system comes in existence. Digital Watermarking is the technique which allows an owner to add hidden copyright notices, image, and signature, audio, video or other messages to digital media. If the media is copied by unauthorized user, then the information embedded in digital media is also carried in the copy. Image watermarking means to embed visible or invisible information in to image that identify the genuine owner. Several techniques for embedded watermark into digital media have been developed so far each of which has its own advantages and limitations, my research work deals with developing the watermarking scheme for digital images. Here we deal with invisible watermarking. Here the main focus is given on better image quality and to retain the integrity of the watermark after being embedding into the original image and reduce perceptual degradation.

Keywords: watermarking, Bi-orthogonal wavelets, digital watermarking

1. INTRODUCTION

The growth of high speed computer networks and World Wide internet (WWW) have explored means of latest business, scientific, diversion and social opportunities within the kind of electronic commercial enterprise and advertising, messaging, period data delivery, data sharing, collaboration among computers, product ordering, group action process, digital repositories and libraries, internet newspapers and magazines, network video and audio, personal communication and much additional. The price effectiveness of merchandising software within the kind of digital pictures and video sequences by transmission over computer network is greatly increased attributable to the improvement in technology.

1.1 Data Hiding

There are several techniques for information hiding into digital media. They are used for several purposes as well as copyright protection. Two basic methods of information hiding are cryptography and steganography. Cryptography is a widely used method for protecting the digital content of the media. The concept of digital watermarking is derived from steganography. The term steganography means “cover writing” and cryptography means “secret writing”.

1.2 Cryptographic Techniques

1. Symmetric Technique

Symmetric cryptography, also called private-key cryptography, is one of the oldest and most secure encryption methods. The term "private key" comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode it. People can use this

encryption method as either a "stream" cipher or a "block" cipher, depending on the amount of data being encrypted or decrypted at a time. A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed chunks of data. Common symmetric encryption algorithms include Caesar cipher algorithm, Data Encryption Standard (DES), Advanced Encryption Standard (AES) [1], and International Data Encryption Algorithm (IDEA).

2. Asymmetric Technique

Asymmetric or public key, cryptography is, potentially, more secure than symmetric methods of encryption. This type of cryptography uses two keys, a "private" key and a "public key," to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users. In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of cipher text messages, who uses it to decrypt them. Algorithms that use public key encryption methods include RSA.

1.3 Watermarking

Watermarking is the process of computer-aided information hiding in a carrier signal. Watermarks may be used to verify the authenticity or the integrity of the carrier signal or to show the identity of its owner. It is prominently used for tracing copyright infringements and for banknote authentication. Watermarking tries to control the robustness at top priority. This space of application of steganography is understood as Digital Watermarking. Digital watermark could be a message/data/information that is embedded into digital content (audio, video, images or text) which will be detected or extracted later. Such message/data/information principally carries the copyright or possession info of the content. The method of embedding digital watermark info into digital content is understood digital watermarking.

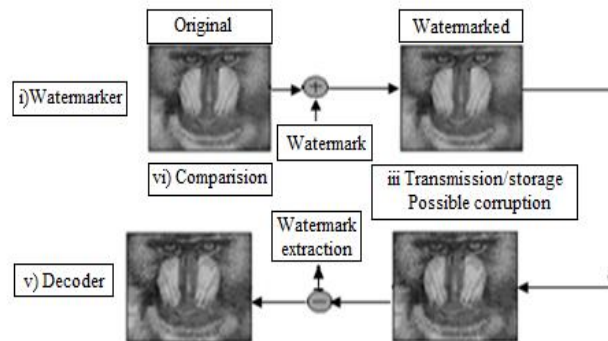


Figure: 1 General watermarking scheme.

1.4 Digital Watermarking

It seems that digital watermarking is a good way to protect intellectual property from illegal copying. It provides a means of embedding a message in a piece of digital data without destroying its value. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music. This chapter focuses on digital watermarking for images and in particular invisible watermarking.

Digital watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or "covered" and graphos or "to write"). A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked.

2 LITERATURE REVIEW

[2] describes some contenders that have appeared in the research literature and in the _eld, In the last few years, a large number of schemes have been proposed for hiding copyright marks and other information in digital pictures, video, audio and other multimedia objects. We then present a number of attacks that enable the information hidden by them to be removed or otherwise rendered unusable. [3] Presents a new watermarking algorithm for digital images. Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia data in a networked environment. It makes possible to tightly associate to a digital document a code allowing the identification of the data creator, owner, authorized consumer, and so on. [4] proposes a novel approach to content-based watermarking for image authentication that is based on Independent Component Analysis (ICA). In the scheme proposed here, ICA is applied to blocks of the host image and the resulting mixing matrix represents the features of the image blocks. Fresenius norm of the mixing matrix is adopted as the content-based feature. This is embedded as the watermark in a mid-frequency DCT coefficient of the block. [5] proposes an entropy based technique for data embedding in images with a specific target, sometimes referred to as feature location: inclusion of a maximum amount of information instead of robustness against attacks. Finally we examine the upper bound of information that can be embedded in the least significant bits by means of our technique and we conclude. [6] Proposed the histogram-based reversible data hiding is limited by the hiding capacity, which is influenced by the overhead of position information that has to be embedded in the host image. To solve this problem, the similarity of neighboring pixels in the images was explored by using the prediction technique and the residual histogram of the predicted errors of the host image was used to hide the secret data in the proposed scheme. [7] Propose a technique can hide an entire image or pattern as a watermark directly into the original image. As the quality of the image is to be preserved the entire image is not altered for embedding, instead few blocks are used based on the size of the watermark and information content of an image block. To reduce the computational complexity of the proposed algorithm Hadamard transformation is used for converting cover image from spatial domain to transform domain. [8] Introduces the entropy masking model in three different domains, and gives experiment report about utilizing spatial domain, DCT domain, and DWT domain entropy masking model in the similar watermarking system. In addition, we analyze the advantages and disadvantages of these models from the aspects of imperceptibility and robustness through our simulation experiment. [9] Proposed a robust watermarking for still digital images based on Fast Walsh-Hadamard Transform (FWHT) and Singular Value Decomposition (SVD) using Zigzag scanning. After applying Fast Wash-Hadamard transform to the whole cover image, the Walsh-Hadamard coefficients are arranged in zigzag order and mapped into four quadrants Q1, Q2, Q3,Q4. These four quadrants represent different frequency bands from the lowest to highest. The quadrant Q1 again divided into non overlapping blocks and in it the highest entropy block is selected and Singular Value Decomposition is applied and the singular values of that block is modified with the singular values of the Fast-Walsh-Hadamard transform and results of the proposed method are found to be superior in terms of imperceptibility and robustness at the expense of increased computational complexity.

3 METHODOLOGIES

The proposed technique is based on interpolation, Entropy calculation, histogram equalization and Bi-orthogonal 2-DWT (discrete wavelet transform) domain. The original image is of 256*256 and watermark should be either equal to size of original image or less than that of the size of original image. The DWT domain improves the security and robustness during communication. The watermark is embedded into the DWT coefficients of the histogram equalized image. In this proposed system firstly I will implement interpolation over the original image using bilinear interpolation; on the interpolated image we apply entropy filtration in order to find which domain is better for embedding the watermark. So we find that out of grey scale, DCT and DWT, DWT domain has highest entropy so for embedding DWT is chosen as it is more

secure and less vulnerable to attacks and the PSNR (peak signal to noise ratio) of the DWT domain over the original image is higher than other domain and. After that we do histogram equalization on the interpolated image to get the histogram equalized image and then we can apply Bi-orthogonal 2-DWT wavelet to insert the watermark. Then again we can decompose the watermark by using BIOR3.5 wavelet and multiply the values of pixels of watermark by the factor alpha in order to insert the watermark uniformly anywhere in the histogram equalized image. The proposed work achieve quite interesting finding.

3.1 Embedding Technique

The watermark is embedded into original image by calculating entropy value so that we can find which area has maximum uncertainty or randomness in order to insert watermark so that it is invisible to others. While embedding we can first improve the quality of image and also remove the pixel errors based on bi-linear interpolation. Following flow chart shows the complete embedding procedure to insert the watermark in to the equalized image:

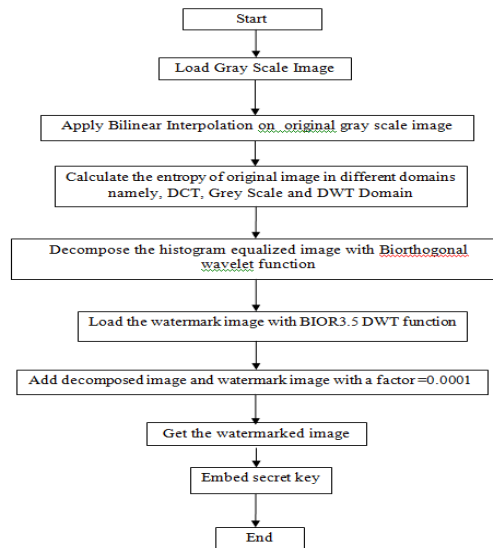


Figure 2: Steps to embed the watermark and to get the watermarked image

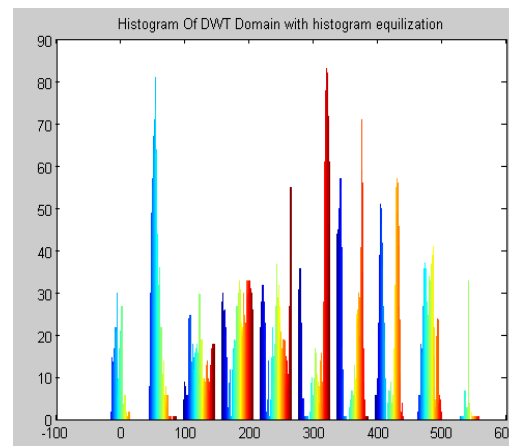


Figure 3: Histogram of equalized image

• Embedding Algorithm

*Step 1: A gray scale original image of 256*256 is chosen and format of any type like png, tiff, and jpg is considered.*

Step 2: Applying interpolation on original image to get interpolated image.

Step 3: Calculate the entropy of the image in different domains i.e gray scale DCT and DWT domain.

Step 4: Now apply a histogram equalization on interpolated image to get a histogram equalized image.

Step 6: Decompose the histogram equalized image using Bi-orthogonal 2-DWT as entropy value is higher in this domain.

Step 7: Also decompose the watermark image with biorthogonal DWT wavelet function.

Step 8: Embedded the watermark into the histogram equalized image by using a Factor=0.0001 to get watermarked image.

Step 9: Now add the secret key into the watermarked image while transferring it over the communication channel.

3.2 Retrieval Technique

For retrieval purpose if the secret key which is embedded or applied to the watermarked image before sending the watermarked image over the public communication channel is known then the watermark is extracted else not. After retrieval we get the image which we insert into the equalized image for copyright protection.

The flowchart depicts the retrieval of invisible watermark from the watermarked image. Watermark is then extracted using inverse of bior3.5 (Bi-orthogonal) DWT wavelet. Retrieving the watermark in such a way that it does not leads to harm the integrity.

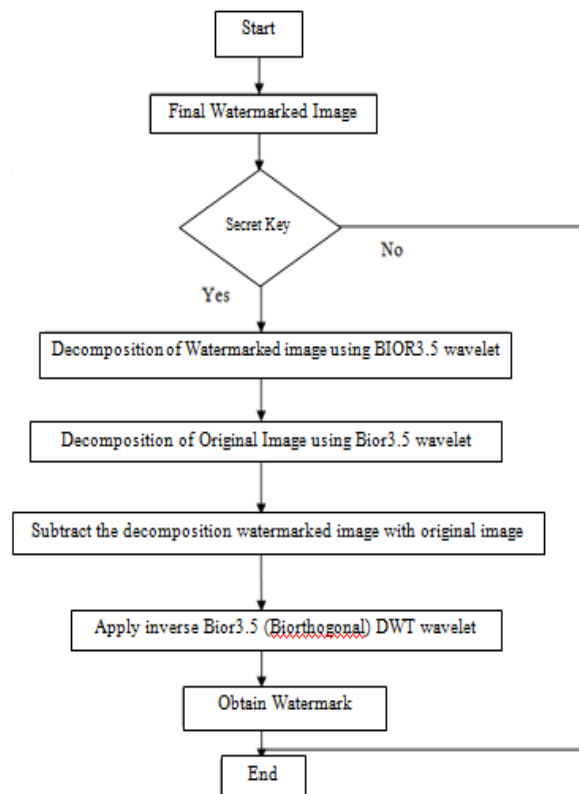


Figure 4: Retrieval Technique

• Retrieval Algorithm

Step 1: Receive the watermarked image through public channel
Step 2: Enter the secret key to extract the watermark. If entered key is incorrect than watermark is not extracted else go to step 3.
Step 3: Decomposed the watermarked image with Bior3.5 wavelet.
Step 4: Also decomposed the histogram equalized image with Bior3.5 wavelet.
Step 5: Subtract the watermarked image with histogram equalized image.
Step 6: Applying bior3.5 DWT on subtracted outcome
Step 7: Finally display the watermark.

4 RESULTS

The proposed algorithm dealt with image watermarking. This technique is applied to grey scale images of size 256*256 and is of the image format png, tiff, bmp, jpg. Also the watermark which is to be embedded is of the size equal to or less than that of the size of original image. This technique is applied to the different images and the same watermark image. The proposed technique can hide entire watermark directly in to the equalized image and retain the integrity of the watermark image after being embedded into the original image. Information is hidden in DWT coefficients which results in less computation time and more security and more invisibility. The evaluation of the algorithm is calculated in terms of PSNR and MSE and the research has resulted in a good PSNR (Peak Signal to Noise Ratio), value and enhanced security with the help of secret key. The aid of watermarking has made this technique more secure for public communication channel. The watermark is used to identify the owner and provide protection to the contents against being copied. Any intruder trying to interfere in between the transmission will neither be able to alter, nor trying to copy the contents. Technique used here the entropy to check maximum randomness area which guarantees maximum invisibility and is less vulnerable to attacks. The quality of image is also increased by histogram equalization technique.

4.1 Performance Analysis

- 1) For the performance analysis we use images of Lena, mandrill, pirate, living room as original image and mandrill as watermark image.
- 2) For the performance analysis we use different original images and same watermark image of Mandrill to get the watermarked image and comparing the PSNR and MSE of different

Original and watermark image as shown in table 1. Here the interpolation error is removed first that estimate the missing pixels in high-resolution from the pixels in low-resolution

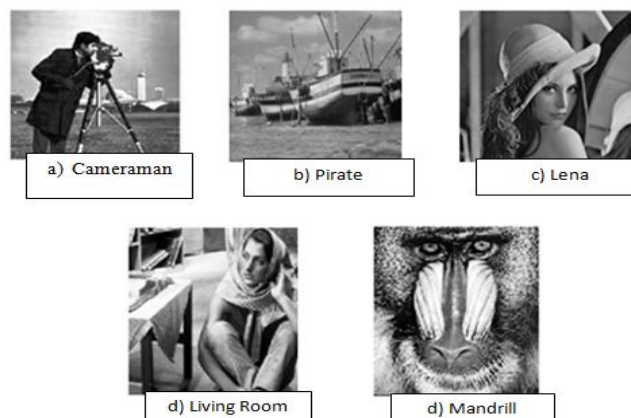














Figure 5: ((a)-(d)) are the original images and (e) watermark images

- 3) For the performance analysis we use different original images and same watermark image of Mandrill to get the watermarked image and comparing the PSNR and MSE of different original and watermark image as shown in table 5.1. Here the interpolation error is removed first that estimate the missing pixels in high-resolution from the pixels in low-resolution. Then enhance the image quality after that find the domain then same images are used to check the different value of PSNR (peak signal to noise ratio) to check the quality of image and MSE (mean square error) between the original and the watermarked image. By applying histogram based technique we get different values of PSNR and MSE. The below table shows that maximum PSNR value comes while we insert the mandrill as a watermark into the histogram equalized image of boat and also the value of MSE is lowest in this case.

Table 1: MSE and PSNR comparison of original images with watermark image

Serial No.	Original Image	Watermark Image	Final Watermark Image	PSNR	MSE
1				88.18	2.96
2				86.41	3.15
3				88.17	2.77
4				84.66	3.69

- 4) Figure 6 the graphical representation of PSNR of different images with same watermark of mandrill. The values are taken from the table 2 to represent the graph. The PSNR is found by taking original images of Lena, cameraman, living room, pirate and watermark image of Mandrill. The horizontal axis shows the original images and vertical shows the range of PSNR. The pink line shows the PSNR at different values.

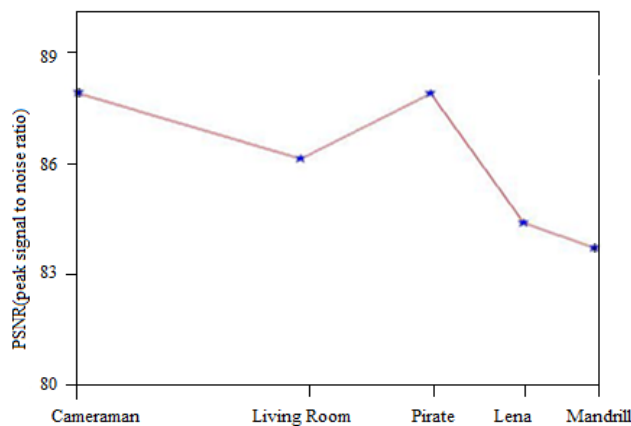


Figure 6: Graphic representation of PSNR

- 5) Figure 7 the graphic representation of MSE of different original images. The MSE is finding by taking original images of Lena, cameraman, Living Room, Pirate, Mandrill and watermark image of Mandrill. The horizontal axis shows the original images and vertical shows the range of MSE. The pink line shows the graphic range of MSE.

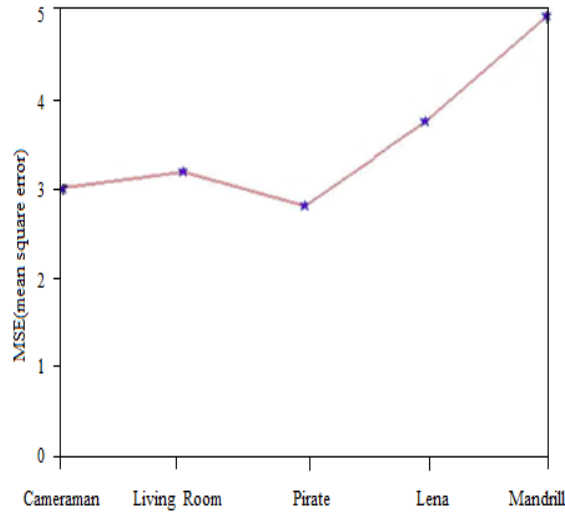


Figure 7: Graphic representation of MSE

- 6) Figure 8 To show the results we take original image of cameraman with watermark A(cameraman) to get watermarked image. This watermarked image is then transmitted over a public communication channel.

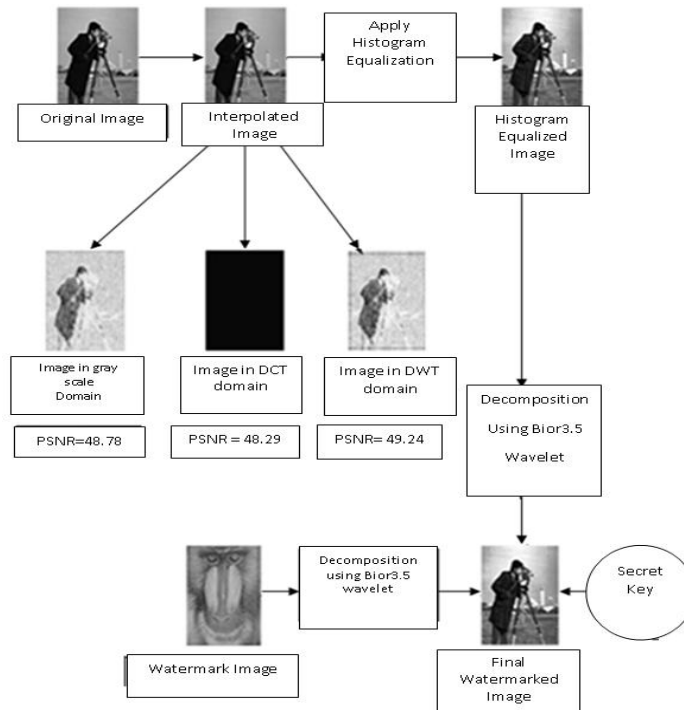


Figure 8: Image Watermark embedding

Figure 9 is showing the extracted watermark image of Mandrill extracted from the watermarked image.

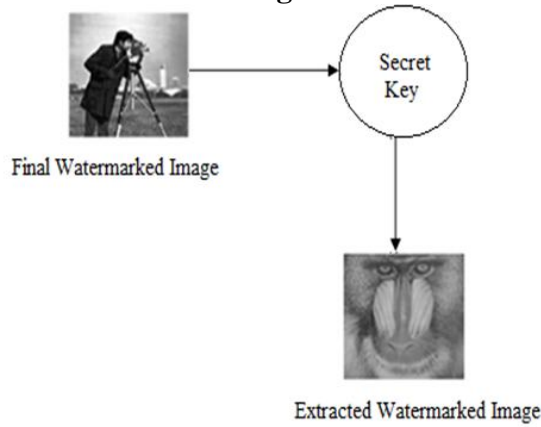


Figure 9 Image watermark extraction

- 7) The Mean Square Error (MSE), PSNR of original image by adding different type of noise like Gaussian, Sparkle, salt and pepper and Poission in different domains like DWT, DCT and Gray scale are compared as shown in table 2.

Table 2 Comparison of different domains by adding different type of noise

Noise Parameters		Gaussian	Sparkle	Salt and pepper	Poission
		Gray Scale	MSE	1.64698	1.64417
PSNR	49.0593		49.0763	48.785	49.0095
DCT domain	MSE	1.77839	1.77844	1.77757	1.77816
	PSNR	48.2916	48.2913	48.2900	48.2929
DWT domain	MSE	1.52469	1.51946	1.6165	1.54086
	PSNR	49.865	49.865	49.246	49.7257

- 8) Comparison result in terms of quality for Lena, Mandrill, Pirate and Living Room. The proposed approach is compared with Existing System[34] show our better results as specified below.

Table 3 Comparison result in terms of quality

Images	Existing System[34]	Proposed work
Lena	61.4094	84.5226
Mandrill	66.1364	81.85
Pirate	67.1234	87.1834
Living Room	64.541	86.2289

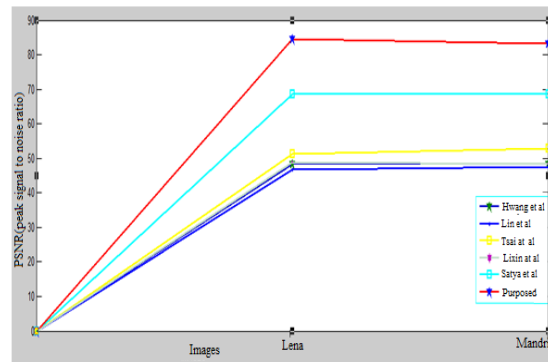


Figure 10 Comparison graph in terms of quality (PSNR).

As the PSNR is compared and it is found that our work is better. It is proved analytically and shown experimentally that the peak signal to noise ratio (PSNR) of the watermarked image versus original image is guaranteed to be above 80 db.

5 CONCLUSIONS

The watermarking is used to transfer copyright information over open channel. The technique proposed here is based on interpolation, histogram equalization, entropy filtration and Bior3.5 DWT. The number of MSBs of payload to be embedded in the cover image based on DCT coefficients. The original image is of 256×256 and converted into DWT coefficients for embedding process. The invisible watermark is added to the original image to make it more protected. The integrity of the data embedded in the original image retains. It is observed that the proposed techniques comes up with a good PSNR (Peak Signal to Noise Ratio), MSE (Mean square error) values and enhanced security and also the secret key by the user or authorized person is added and is used at another side when one want to extract the hidden data (watermark) from the original image. If anyhow the key entered by the user is wrong then user is not able to extract the watermark. Any intruder cannot find that there is some watermark is added into the original image and when trying he/she fails and would not be able to copy it or extract anything.

In chapter 4, we discuss the methodology we adopted here for the implementation of proposed algorithm. And in chapter 4, we discuss the results of our proposed algorithm and findings shows that as far as existing literature is concerned, we have achieved better quality. We have used Bior3.5 wavelet for decomposition of the image and provide much better results. Also we have calculated PSNR for different values of alpha and finding shows that at value of $\alpha=0.0001$, the PSNR of image is maximum.

REFERENCES

1. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
2. [David Aucsmith "Self-Similarity Based Image Watermarking", 9th European Signal Processing Conference, Island of Rhodes, Greece, Page 2277 – 2280, ISBN 960 – 76204-05, 11 April. 1998.
3. Mauro Barni, Franco Bartolini "A Dct Domain System For Robust Image Watermarking" *Eurasip*, Vol. 66, No. 3, P357-372, May 1998.
4. Latha Parameswaran, K. Anbumani, "Content-Based Watermarking For Image Authentication Using Independent Component Analysis" 6TH ACM Multimedia, England, P61 – 70, Sept 1998.
5. Marc VAN DROOGENBROECK & Jérôme DELVAUX," An entropy based based technique for information embedding in images ", IEEE Benelux Signal Processing Symposium (SPS-2002), Leuven, Belgium, March 21–22, 2002.
6. P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, 2009.
7. Franklin Rajkumar, V Manekandan & GRS V.Santhi," Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique", *International Journal of Computer Applications* , Volume 12– No.9, January 2011.
8. Qiu Yang, Yana Zhang & Cheng Yang, Wei Li," Information entropy used in digital watermarking", *IEEE trans*, 2012.
9. K.Mccnakshi, Ch.Srinivasa Rao, K.Satya Prasad" A Robust watermarking scheme based on Walsh-Hadamard Transform and SVD using Zig-Zag Scanning" *Master Thesis, and International Conference on Information Technology*, 2014.