International Journal For Technological Research In Engineering
Volume 1, Issue 7, March-2014 *ISSN (Online): 2347 - 4718*

ROBUST IMAGE WATERMARKING

Savsani Deepkumar Mansukhlal[1], Hansaliya Rishit Nileshbhai[2], Kantaria Parth Ratilal[3],
Patel Unnati Bhupendra[4], Tejpal Jhajharia[5]
[1,2,3,4] M.Tech Student, [5]Assistant Professor I
[1,2]Department of Electronics & Communication Engineering, Manipal University Jaipur, Rajasthan, India
[3]Department of Electronics & Communication Engineering, R.K University, Gujarat, India
[4]Department of Electronics & Communication Engineering, GTU PG School, Gandhinagar, Gujarat, India
[5]Department of Electronics & Communication Engineering, Manipal University Jaipur, Rajasthan, India

***Abstract*: The 21st century has seen a very great impact of the rising technology. The major problem that is being faced is the security issue since Hacking of the sensitive documents is widely increased. In order to increase the security in Intellectual Property Rights (IPR) protection, Demonstration of rightful ownership, Authentication, Labeling for data retrieval this can be implemented. Digital watermarking technology has been actively studied and developed by a number of institutions and companies since mid '90s. The digital watermarking is very much needed in this technological era. According to the characters of human vision, in this algorithm, the information of digital watermarking which has been discrete wavelet transformed, is put into the high frequency band of the image which has been wavelet transformed. Then distills the digital watermarking with the help of the original image and the watermarking image. The simulation results show that this algorithm provides an excellent watermarking and also good robustness for some common image processing operations.**

In practical applications, the image may go through a number of attacks during the transmission of the image over a network but with the help of this algorithm, the authentication of the image can be easily done. Our analysis and results shows that this watermarking algorithm is much efficient than the existing algorithm. This proves that the algorithm is efficient and can survive many attacks.

***Keywords:* Matlab 7, Adobe Photoshop, Hard Disk, RAM, Graphic card.**

I. INTRODUCTION

The last decade has witnessed the rapid development in information technologies and the wide availability of digital consumer device such as digital cameras, scanners etc. But at the same time this leads to the hacking vulnerability and duplicity of the original information. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of this concept in the digital world. In recent years, the rapid growth of the Internet has highlighted the need for mechanisms to protect ownership of digital media. Watermarking is a relatively new and unexplored field in which extensive research is going on all over the world and it has the potential to provide simple and easily implementable solution to provide rightful ownership.

II. SYSTEM ANALYSIS

Mathematical transformation is applied to signals to obtain further information from that signal that is not readily available in the raw signal. Often times, the information that cannot be readily seen in the time domain can be seen in frequency domain.

Although FT is probably the most popular transform being used, it is not the only one. There are many other transform that are used quite often by Engineers and mathematicians. Hilbert transform, short time Fourier transform, Wigner distributions, the radon Transform. The Wavelet Transform, constitute only a small portion of huge list of transform that are available at Engineering's and mathematician's disposal. Every transforms technique has its own area of application with advantages and disadvantages.

A. Fourier Analysis

Fourier analysis is a subject area which grew from the study of Fourier series. The subject began with the study of the way general functions may be represented by sums of simpler trigonometric functions. Fourier analysis is named after Joseph Fourier, who showed that representing a function by a trigonometric series greatly simplifies the study of heat propagation.

Today, the subject of Fourier analysis encompasses a vast spectrum of mathematics. In the sciences and engineering, the process of decomposing a function into simpler pieces is often called Fourier analysis, while the operation of rebuilding the function from these pieces is known as Fourier synthesis. In mathematics, the term Fourier analysis often refers to the study of both operations.

B. Short-time Fourier Analysis

The short-time Fourier transform (STFT), or alternatively short-term Fourier transform, is a Fourier-related transform used to determine the sinusoidal frequency and phase content of local sections of a signal as it changes over time.

C. Wavelet Analysis

A wavelet is a wave-like oscillation with amplitude that starts out at zero, increases, and then decreases back to zero. It can

Copyright 2013.All rights reserved.

typically be visualized as a "brief oscillation" like one might see recorded by a seismograph or heart monitor. Generally, wavelets are purposefully crafted to have specific properties that make them useful for signal processing. Wavelets can be combined, using a "revert, shift, multiply and sum" technique called convolution, with portions of an unknown signal to extract information from the unknown signal.

As a mathematical tool, wavelets can be used to extract information from many different kinds of data, including - but certainly not limited to - audio signals and images. Sets of wavelets are generally needed to analyze data fully. A set of "complementary" wavelets will deconstruct data without gaps or overlap so that the deconstruction process is mathematically reversible. Thus, sets of complementary wavelets are useful in wavelet based compression/decompression algorithms where it is desirable to recover the original information with minimal loss.

D. Discrete Wavelet Transform

A discrete wavelet transform is any wavelet transform for which the wavelets are discretely sampled. Discrete Wavelet Transform, which is based on sub-band coding, is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. The foundations of Discrete Wavelet Transform go back to 1976 when techniques to decompose discrete time signals were devised.

In Continuous wavelet transform, the signals are analyzed using a set of basic functions which relate to each other by simple scaling and translation. In the case of Discrete Wavelet Transform, a time-scale representation of the digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales.

Watermarking scheme based on the Discrete Wavelet Transform. The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image.For 2-D images, applying Discrete Wavelet Transform corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution coefficient sets, a lower resolution approximation image (LL1) as well as horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components as shown in the figure below. The sub-band LL1 represents the coarse-scale Discrete Wavelet Transform coefficients while the coefficient sets LH1, HL1 and HH1 represent the fine-scale of Discrete Wavelet Transform coefficients as shown in the figure 1.

E. Wavelet Families

There are a number of basic functions that can be used as the mother wavelet for Wavelet Transformation. Since the mother wavelet produces all wavelet functions used in the transformation through translation and scaling, it determines the characteristics of the resulting Wavelet Transform. Therefore, the details of the particular application should be taken into account and the appropriate mother wavelet should be chosen in order to use the Wavelet Transform effectively.

(1) Haar (2) Daubechies (3) Coiflet (4) Mexican Hat.

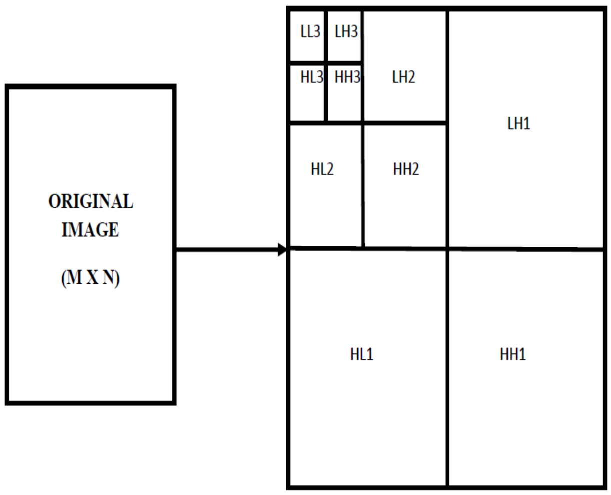


Fig.1. n-Level Wavelet Decomposition.

F. Haar

Haar wavelet is a sequence of rescaled "square-shaped" functions which together form a wavelet family or basis. Wavelet analysis is similar to Fourier analysis in that it allows a target function over an interval to be represented in terms of an orthonormal function basis.

The Haar wavelet as shown in the figure 2 is also the simplest possible wavelet. The technical disadvantage of the Haar wavelet is that it is not continuous, and therefore not differentiable. This property can, however, be an advantage for the analysis of signals with sudden transitions, such as monitoring of tool failure in machines.

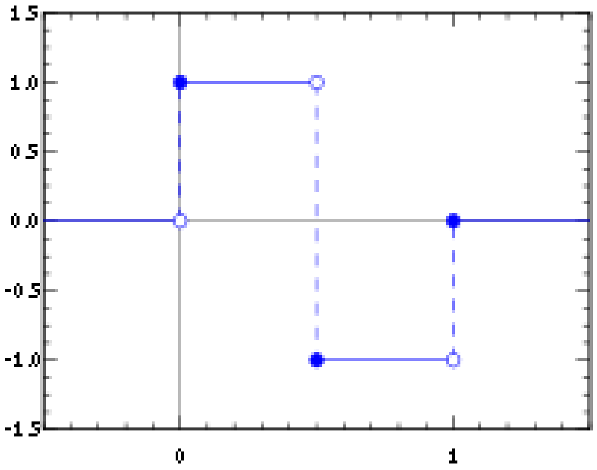


Fig.2. Haar Wavelet.

G. Daubechies

The Daubechies wavelets, named after Ingrid Daubechies are a family of orthogonal wavelets defining a discrete wavelet transform and characterized by a maximal number of vanishing moments for some given support. With each wavelet type of this class, there is a scaling function (also called father wavelet) which generates an orthogonal multi-resolution analysis. This is clearly explained in the figure 3.

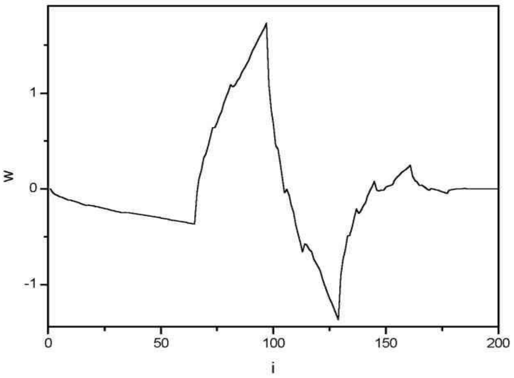


Fig.3. Daubechies Wavelet.

H. Coiflets

Coiflets are discrete wavelets having scaling functions with vanishing moments. The wavelet is near symmetric, their wavelet functions have N/3 vanishing moments and scaling functions N/3 -1 and have been used in many applications using Calderón-Zygmund Operators. The figure 4 describes the Coiflet wavelet.

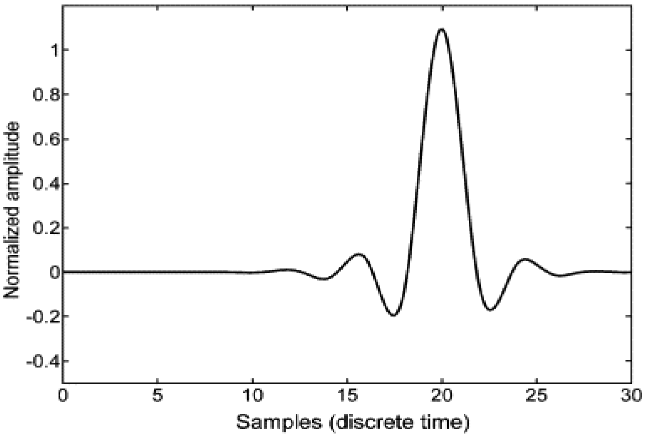


Fig.4. Coiflets Wavelet

I. Mexican hat

This wavelet has no scaling function and is derived from a function that is proportional to the second derivative function of the Gaussian probability density function.

The figure 5 describes the Mexican hat wavelet. Here we can notice that there is a increase and variation as the values increases. It reaches to 0.8 and decreases once it reaches the mean value.

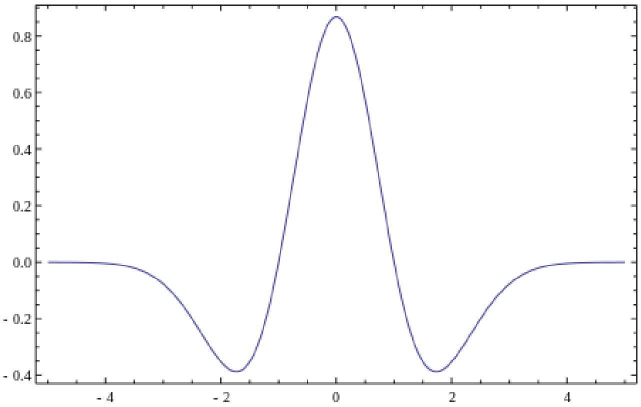


Fig.5. Maxican Hat Wavelet.

J. Discrete Cosine Transform (DCT)

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer functions are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

K. Singular Value Decomposition (SVD)

The singular value decomposition (SVD) is a factorization of a real or complex matrix, with many useful applications in signal processing and statistics. The singular value decomposition of an $m\times n$ real or complex matrix M is a factorization of the form;

$$\mathbf{M = U \Sigma V^{*,}}$$

where U is an $m\times m$ real or complex unitary, Σ is an $m\times n$ rectangular diagonal matrix with nonnegative real numbers on the diagonal, and V^* (the conjugate transpose of V) is an $n\times n$ real or complex unitary matrix. The diagonal entries $\Sigma_{i,i}$ of Σ are known as the singular values of M. The m columns of U and the n columns of V are called the left singular vectors and right singular vectors of M, respectively.

The singular value decomposition and the Eigen decomposition are closely related. Namely:

- The right singular vectors of *M* are eigenvectors of M*M
- The left singular vectors of *M* are eigenvectors of MM *
- The non-zero singular values of *M* (found on the diagonal entries of Σ) are the square roots of the non-zero eigen values of both MM *and M*M.

Applications which employ the SVD include computing the pseudo inverse, least squares fitting of data, matrix approximation, and determining the rank, range and null space of a matrix.

III. SYSTEM DESIGN

General digital watermarking processes are embedding, attacking, and detection retrieval functions. The information to be embedded is an image is called a digital watermark. The image where the watermark is to be embedded is called original image.

The image that has to be watermarked is taken and is subjected into the Discrete Wavelet Transform. After the original image has been Discrete Wavelet Transform transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. Decompose the host image by using two-dimensional Discrete Wavelet Transform.

A watermarking system is usually divided in to three distinct steps, embedding, attack, and detection as depicted in figure 6.

The watermark image that has to be embedded should be resized to the size of the original image so that the watermark image can be embedded into the original image. This resized watermark is decomposed into 4 frequency coefficients using Discrete Wavelet Transform. Later, using the algorithm, the watermark is successfully embedded into the original image. The Peak Signal to noise ratio is then calculated. Now, the watermarked image is ready for use.

This watermarked image undergoes a series of attacks to check its robustness. The image after the attack, is taken and the watermark is extracted. The Correlation Coefficient is later found. The Correlation Coefficient is a measure of how well the predicted values from a forecast model "fit" with the real-life data. It calculated between the extracted watermark image and the embedded watermark. The correlation coefficient is a number between 0 and 1. If there is no relationship between the predicted values and the actual values the correlation coefficient is 0 or very low. Thus the higher correlation coefficient the better.

IV. IMPLEMENTATION

In this project the one powerful frequency domain namely, Discrete Wavelet Transform is used to embed the watermark information in the image. The proposed Discrete Wavelet Transform watermarking algorithm consist of two procedures; the first embeds the watermark into the cover image, while the other extracts it from the watermarked version of image. The block diagram of the proposed system is shown in figure 7.

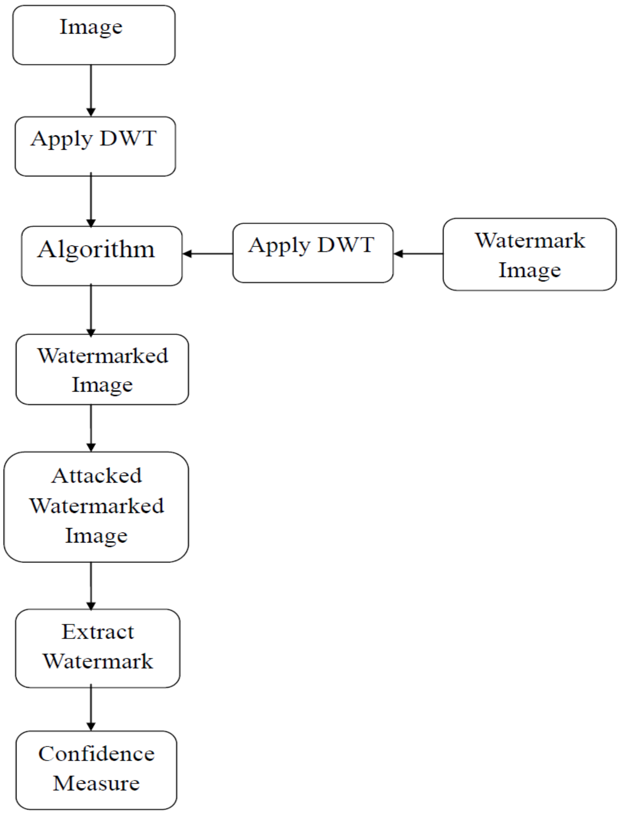


Fig.6. Digital Watermarking Proposed system.

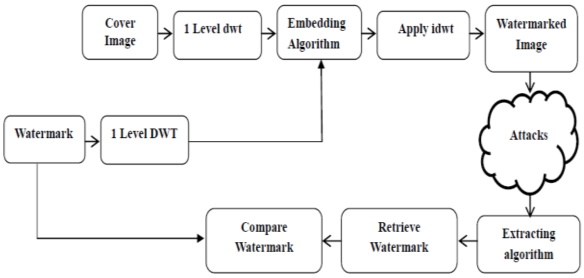


Fig.7. Block diagram of Discrete Wavelet Transform watermarking Process.

The image that has to be watermarked is taken and is subjected into the Discrete Wavelet Transform. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district as shown in the figure 5.1. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency coefficient(LL) and three high-frequency coefficients (LH,HL,HH). If the information of

Copyright 2013.All rights reserved.

low-frequency coefficient is DWT transformed, the sub-level frequency coefficient information will be obtained. Decompose the host image by using two-dimensional Discrete Wavelet Transform.

The watermark image that has to be embedded should be resized to the size of the original image so that the watermark image can be embedded into the original image. This resized watermark is decomposed into 4 frequency coefficients using Discrete Wavelet Transform. Later, using the algorithm, the watermark is successfully embedded into the original image. The Peak Signal to noise ratio is then calculated. Now, the watermarked image is ready for use.

This watermarked image undergoes a series of attacks to check its robustness. The image after the attack, is taken and the watermark is extracted. The Correlation Coefficient is later found. The Correlation Coefficient is a measure of how well the predicted values from a forecast model "fit" with the real-life data. It calculated between the extracted watermark image and the embedded watermark. The correlation coefficient is a number between 0 and 1. If there is no relationship between the predicted values and the actual values the correlation coefficient is 0 or very low. Thus the higher correlation coefficient the better.

V. TESTING AND RESULT ANALYSIS

The performance of the proposed DWT based watermarking method is evaluated with respect to three metrics Imperceptibility, Robustness, and payload.

A. Imperceptibility

Imperceptibility means that the perceived quality of the image should not be distorted by the presence of the watermarking. As a measure of the quality of the watermarked image, the Peak Signal to Noise Ratio (PSNR) is typically used as shown in equation 6.1. We obtain a high PSNR value of 42.1 dB which proves the imperceptibility.

PSNR = 10 * log10 (256^2 / mse)

Where MSE is mean square error.

B. Robustness

Robustness is a measure of the immunity or resistance of the watermark against attempts to remove or degrade it by different types of Digital Signal Processing Attacks.

The similarity between the original watermark and the extracted watermark from the attacked watermarked images was measured using the MATLAB correlation coefficient.

A correlation co-efficient of 1.0 is obtain from the equation 6.2, which shows the exact matching between the original and the extracted watermark.

The results demonstrate that the propose method achieved good robustness for different types of attacks. The propose scheme is also tested for various images and different watermark images.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}}$$

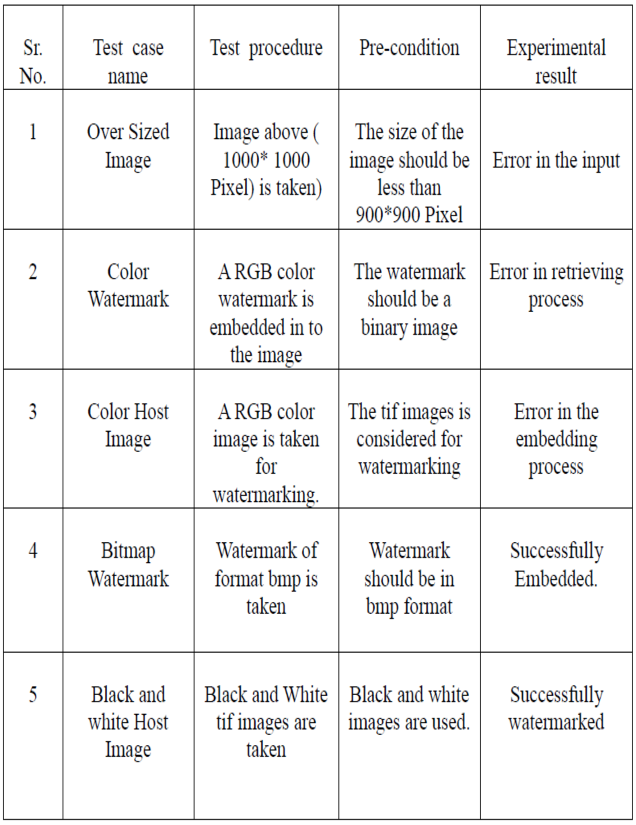
where $\bar{A}$ = mean2(A), and $\bar{B}$ = mean2(B).

The results demonstrated that this schemes achieve good imperceptibility, but demonstrated the fragility when subjected to various attacks. Recovery of the watermark image for various attacks is not satisfactory. For demonstration purpose only Gaussian noise attack is shown

C. Payload

Data payload or watermarking capacity for a given image is define as the number of watermark bits that can be embedded into the cover image without causing any visual distortion in the image. The proposed algorithm restricts the payload to be maximum size of the length of diagonal elements of Horizontal components. However the payload can be increased if embedding is done in Vertical and Diagonal components also.

Test case table is shown with the different test cases in table 1.



Sr. No.	Test case name	Test procedure	Pre-condition	Experimental result
1	Over Sized Image	Image above (1000* 1000 Pixel) is taken)	The size of the image should be less than 900*900 Pixel	Error in the input
2	Color Watermark	A RGB color watermark is embedded in to the image	The watermark should be a binary image	Error in retrieving process
3	Color Host Image	A RGB color image is taken for watermarking.	The tif images is considered for watermarking	Error in the embedding process
4	Bitmap Watermark	Watermark of format bmp is taken	Watermark should be in bmp format	Successfully Embedded.
5	Black and white Host Image	Black and White tif images are taken	Black and white images are used.	Successfully watermarked

Table.1. Test case with different Images.

The first test case takes an input of an over-sized image which gives an error report since matlab does not support image of higher value. The second test case take an input of a color watermark image which does not support since binary watermarks are considered here. The third test case takes an input of a color host image and exhibits an error since the algorithm supports only the tif formatted images. The last two test cases shows the positive result when the binary watermark image and black and white image is taken as input.

VI. SCREEN LAYOUT

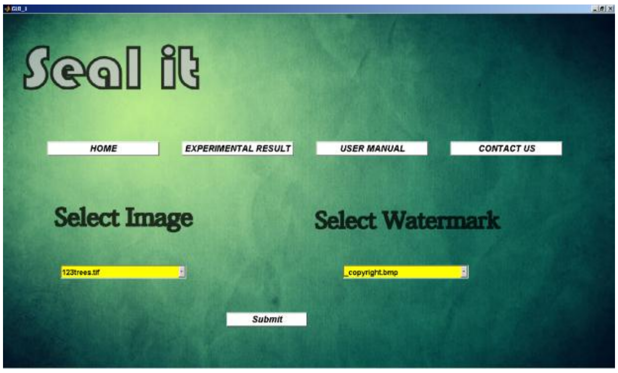
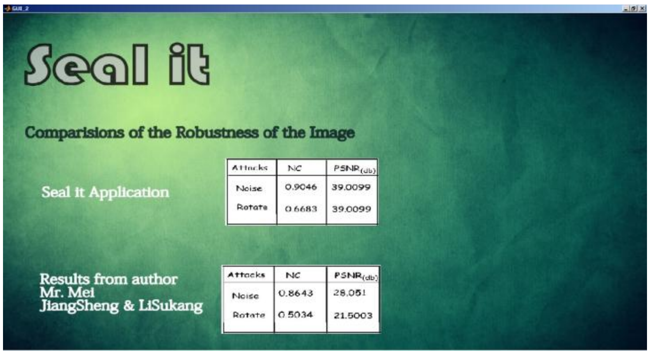


Fig.8. Home Page

The figure 8 describes the home page of the application contains five buttons namely ‘Home’, ‘Experimental Result’, ‘User manual’, ‘contact us’ and ‘Submit’



Comparisions of the Robustness of the Image

Seal it Application

Attacks	NC	PSNR(db)
Noise	0.9046	39.0099
Rotate	0.6683	39.0099

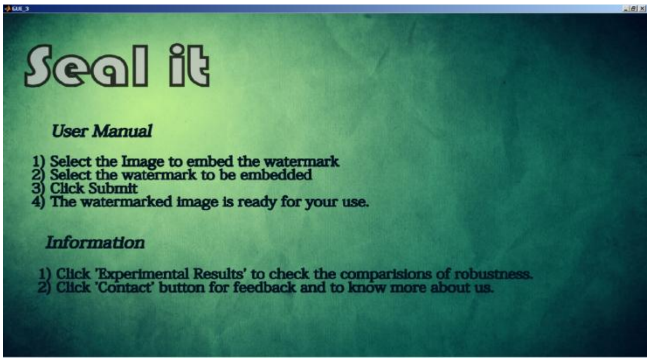
Results from author Mr. Mei JiangSheng & LiSukang

Attacks	NC	PSNR(db)
Noise	0.8643	28.051
Rotate	0.5034	21.5003

Figure 9 Experimental result.

The table compares the peak signal to noise ratio and Numberical coeffciecnt between the seal it application and of the author as shown in the figure 9.
The figure 10 describes the user manual which contains the instruction about how to use the application.

The figure 10 describes the user manual which contains the instruction about how to use the application.



User Manual

1) Select the Image to embed the watermark
2) Select the watermark to be embedded
3) Click Submit
4) The watermarked image is ready for your use.

Information

1) Click ‘Experimental Results’ to check the comparisions of robustness.
2) Click ‘Contact’ button for feedback and to know more about us.

Figure 10 User Manual.

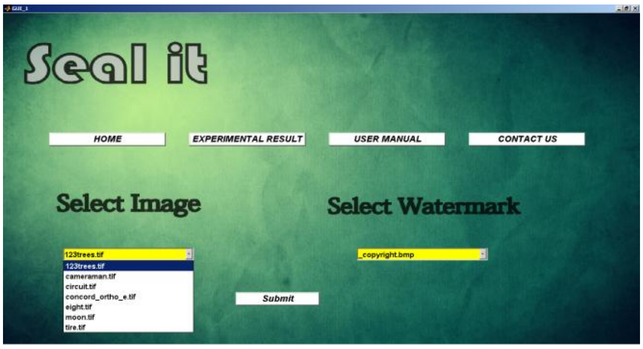


Figure 11 Select Original Image.

The Image is selected that has to be watermarked from the list of images that are required by the user as shown in the figure 11.

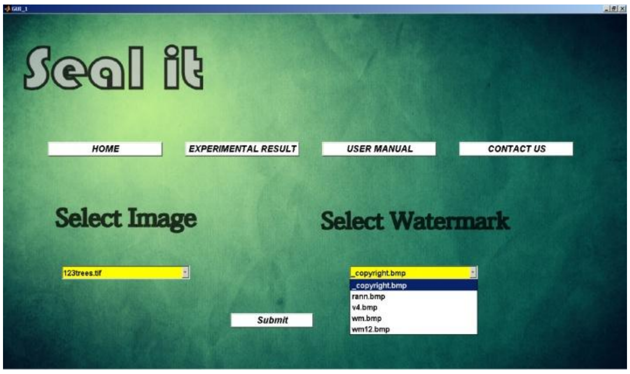


Fig.12. Select Watermark

The figure 12 describes that the watermark that has to be embedded has to be selected from the list of the images that are provided.

The host image that is taken for watermarking is displayed as shown in the figure.

Copyright 2013.All rights reserved.

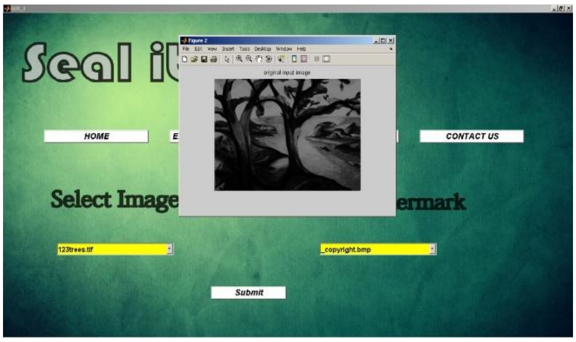


Fig.13. Original Image.

The Discrete wavelet transformation is applied to the image and it divides the image based on the frequency as shown in the figure 14.

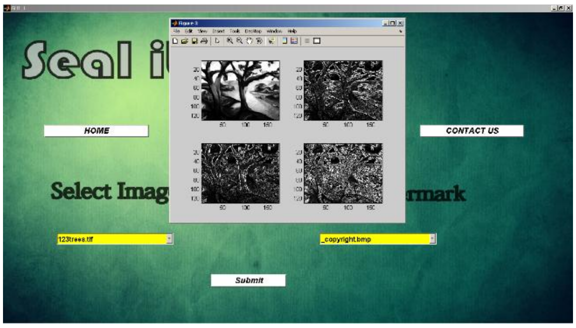


Fig.14. DWT Applied Image.

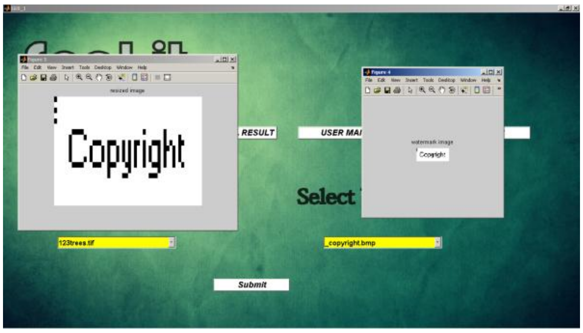


Fig.15. Resized Watermark Image.

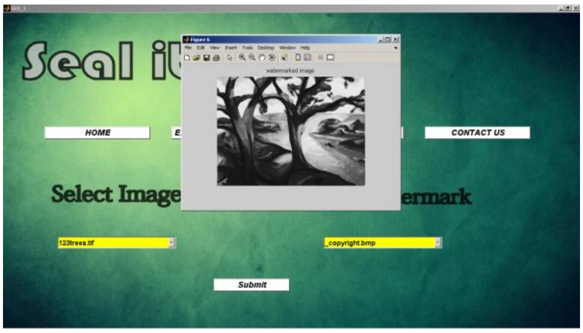


Fig.16. Watermarked Image.

The figure 15 describes how the watermark image that a is taken is resized to the size of the host image

The Image that is watermarked is displayed. This watermarked image looks exactly the same like that of the host image as shown in the figure 16

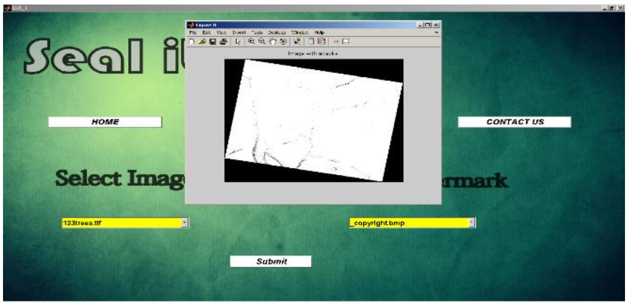


Fig.17. Watermarked Image Rotated at 20^0 Degree.

The watermarked image may have to undergo a lot of attacks. Here is the example of the rotate attack which makes the image rotated at 20^0 Degree.

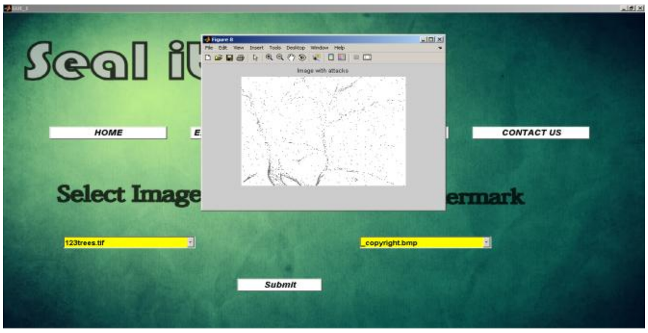


Fig.18. Salt-Pepper Noise added Watermarked Image.

The figure 18 describes how the watermarked image is attacked by adding noise into the image. Here, the Salt-Pepper noise is added into the image.

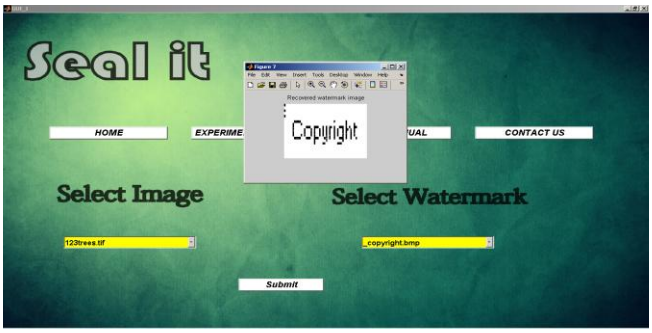


Fig.19. Retrieved Watermark Image.

The watermark that is embedded is retrieved from the host image for the purpose of authentication is shown in the figure 19.

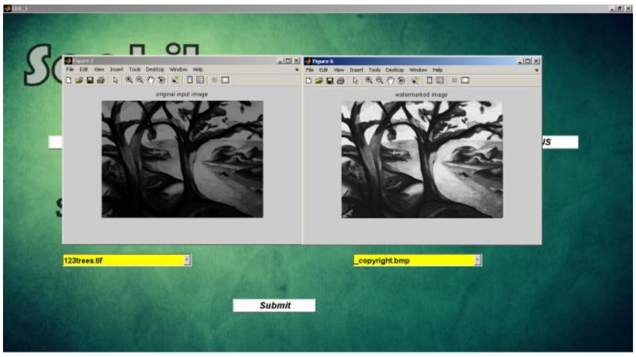


Fig.20. Comparison of Original and Watermarked Image.

This snapshot shows the comparison of the original image and the watermarked image which appears same as shown in the figure 20.

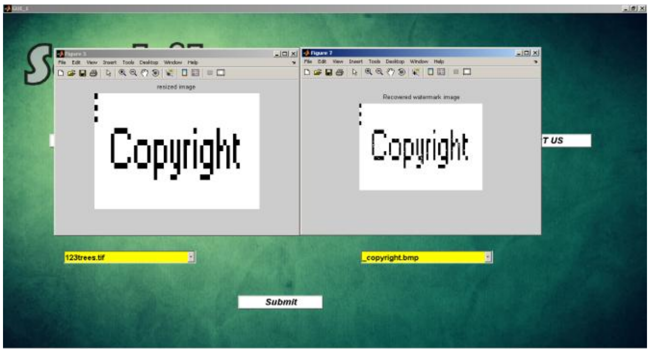


Fig.21. Comparison of Original and Retrieved Watermarked Image.

The figure 21 describes how the watermark embedded on to the host image is compared with retrieved watermark.

VII. CONCLUSION AND FUTURE ENHANCEMENT

The Digital image watermarking has made a great impact in this era. Here we have proposed a robust image watermarking technique that survives from most of the malicious manipulations. In practical applications, the image may go through a number of attacks but with the help of this algorithm, the authentication of the image can be easily done. Our analysis and results shows that this watermarking algorithm is much efficient than the existing algorithm. This proves that the algorithm is efficient and can survive many attacks which makes it robust.

A common application requirement for the watermarks is that they resist attacks that would remove it. Some of the watermarks being attack-resistant may be accidentally removed by unintended attacks such as cropping, reduction, or compression. There are also other techniques like blind watermarking (which uses multiple watermarks and also no need of original image at the of watermark recovery), which uses watermark nesting and encryption. Nesting means it embeds an extra watermark into the main watermark and then embeds the main watermark into the cover image.

The present work can be extended for Video Watermarking and is in progress. Further the payload restrictions can be solved by taking multilevel Discrete Wavelet Transform embedding in all the sub-bands of Discrete Wavelet Transform coefficients.

REFERENCES

[1] Mrs. Neeta Deshpande, Dr. Archana rajurkar, Dr. R. manthalkar, “Review of Robust Video Watermarking Algorithms” By in International Journal of Computer Science and Information Security,Vol. 7, No. 3, March 2010.

[2] Alexander Hasslacher, “Digital Watermarking” 0056448 EMT-Institute, JKU-Linz, 2004

[3] Emir Ganic and Ahmet M. Eskicioglu Department of Computer and Information Science CUNY Brooklyn College, “ROBUST EMBEDDING OF VISUAL WATERMARKS USING DWT-SVD” By 2900 Bedford Avenue Brooklyn, NY 11210, USA.

[4] Tahani Al-Khatib, Ali Al-Haj, Lama Rajab and Hiba Mohammed The University of Jordan, Al-Jubeiha, “A Robust Video Watermarking Algorithm” 2008 Science Publications.

[5] Amit Phadikar, “ROBUST WATERMARKING TECHNIQUES FOR COLOR IMAGES”

[6] Norishige Morimoto IBM Japan “Digital Watermarking Technology with Practical Applications”, Tokyo Research Laboratory in 1999.

[7] Dr. Mohammed Al- ualla and Prof. Hussain Al-Ahmad, Multimedia Communication and Signal Processing, “Information Hiding: Steganography and Watermarking”.

[8] Mei Jiansheng, Li Sukang and Tan Xiaomei Nanchang Power Supply Company,Nanchang, China, Nanchang, P. R. China “A Digital Watermarking Algorithm Based On DCT and DWT” By, May 22-24, 2009, pp. 104-107.

[9] Rafael C. Gonzales & Richard E. Woods, “Digital image processing”.

[10] Dwijesh Dutta Majumder, “Digital Image Processing and Analysis”.

I.