International Journal Of Core Engineering & Management
Volume-4, Issue-2, May-2017, ISSN No: 2348-9510

A STUDY AND PERFORMANCE EVALUATION OF WATERMARKING TECHNIQUES

Smt.M.Tirupathamma
Assistant Professor, Department of ECE, JNTUHCEJ, Jagtial,
Telangana, India

Abstract

Nowadays securing our information is very difficult. Many new techniques are being developed to secure the data. Watermarking is a technique which is used to hide data or identifying information within digital multimedia. An image can be represented in 3 domains namely spatial, frequency and mixed domain. Hence watermarking can be done in any of the three domains. In spatial domain watermarking, manipulations to the image are made in the spatial domain. One of the prominent spatial domain techniques is LSB substitution technique. In our paper we implement a variation of the LSB substitution technique. We extract bit-planes of the both images and watermark embedding is performed. In frequency domain watermarking, the images are transformed into frequency domain before any manipulations are performed. The transform technique used in this paper is DCT (Discrete Cosine Transform). We develop a technique based on the COX method. In mixed domain watermarking, the images are represented in frequency-time domain. For this conversion of image into mixed domain, we make use of DWT (Discrete Wavelet Transform). The embedding of watermark is done in the mixed domain itself. At last, the performance of all the three watermarking techniques is compared using appropriate performance evaluation tools. We have used MATLAB (matrix laboratory) as our software tool to develop all the watermarking techniques because MATLAB provides a rich class of functions to use for image processing. We have made extensive use of the image acquisition toolbox, image processing toolbox and wavelet toolbox. The functions present in these toolboxes are sufficient enough for every image process.

Keywords: Watermarking, LSB, DCT, DWT, Performance evaluation.

I. INTRODUCTION

Watermarking is a technique which can be used to secure the data in images or videos. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. Because of this extensive use, watermarking techniques are often evaluated based on their invisibility, capacity, and robustness. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked image and the cover image [1]. The image where the watermark is to be embedded is called the cover work. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In the embedding process, the cover image is taken as input and the data to watermarked is sent along with the cover image and

www.ijcem.in

it generates a water marked image[9]. Then the watermarked image is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. When any third person used to remove the water mark thorough the different techniques then the data is not secured. There are many possible modifications, for example, lossy compression of the data, cropping an image or video or intentionally adding noise. The general process in the life cycle of the digital watermarking is shown in the below figure 1.

There some tools to evaluate the performance of the watermarking technique. Some of them are MSE (mean square error), PSNR (peak signal to noise ratio), SSIM (structural similarity) etc. We will be using some of these tools in our paper to evaluate the techniques which we have developed.

This paper develops three watermarking techniques one from each domain. The techniques developed are newest and simple in their respective domains. So we can compare the advantages and disadvantages of each technique and we can choose the appropriate watermarking technique which suits our application. The choice is better made when we consider the performance evaluation tools. All these facilities are provided in this paper. A user can make a choice from the three techniques offered and he can come to a conclusion based on the MSE and PSNR values provided. Hence the importance of this paper is that it develops three new watermarking techniques evaluates each of them and also provides a choice to the user to choose best technique suitable to his requirement.

Section 2 talks about literature review, section 3 discusses about overview of watermarking techniques, section 4 demonstrates implementation of different watermarking techniques, section 5 talks about performance evaluation tools, section 6 discusses about experimental results, and section 7 concludes the paper.

www.ijcem.in

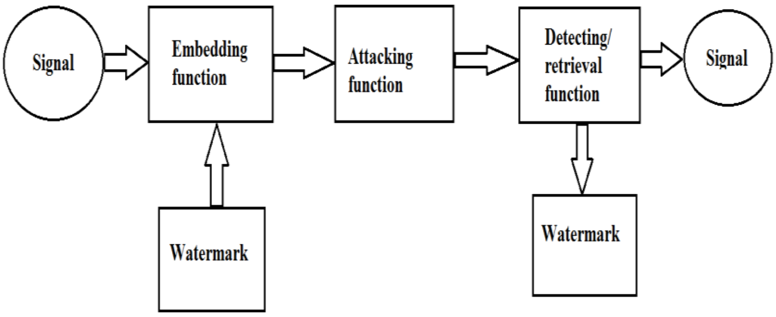


Figure 1: General life cycle of watermarking

II. LITERATURE REVIEW

Image is a stored description of a graphic picture, either a set of brightness and color values of pixels or a set of instructions for reproducing the picture. Now a day, we live in the digital world and the protection of digital content is essential, especially for owners and distributers. The field of digital watermarking provides solutions all these problems. And this field is the choice of research of any budding engineer. Because of there are many new watermarking techniques invented almost every day. Hence digital watermarking is one and only solution to the copyright protection in the near future. Digital watermarking is an information hiding technique which hides information in some file. The information can be text or image or audio or video. In its initial stage, paper watermark appeared in 1282 in Italy when thin wires were added to the paper mold [2]. However, the commercial use of watermark started in 18th century in Europe and America. The use of watermark then extended beyond the scope of paper and was used in other physical objects (fabrics, garment labels, product packaging etc.) and electronic signals (music, photograph, video etc.). Digital watermarking got an extensive popularity in the latter half of 1990s. Initially, informed techniques of watermarking have been used where the original work or any information about the original work is required at the receiving side. In 1997, Piva et al have introduced the blind watermarking technique, where the original or any information about the original work is not required. Now-a-days, most of the researchers are using blind watermarking approaches.

The recent growth in computer networks, and more specifically, the World Wide Web, has allowed multimedia data such as images to be easily distributed over the Internet. on the other side, most of the people are not willingly show their contribution of work on internet due to not having security in internet. Images can be easily duplicated and distributed without the owner's consent like copying the digital contents without any constraints, forgery, and editing without any prohibitive professional efforts. Digital watermarks are the solutions for achieving security. The main reason for development of digital watermarking research is the endeavor for coming up with innovations to protect intellectual properties of the digital world.

A general watermarking system can be divided into three main components:

The watermark signal (W), which is generated with the help of generating function (f_g). Usually the watermark generation depends on a secret key (k) and watermark information (i) and sometimes on cover work (X) also.

$$W = f_g\ (i, k) \text{ or } W = f_g\ (i, k, X)$$

The embedding function (f_m), which incorporates the watermark signal (W), into the cover work (X), and yields the watermarked data (X_w). Typically, the watermark incorporation depends on a key (k),

$$X_w = f_m\ (X, W, k)$$

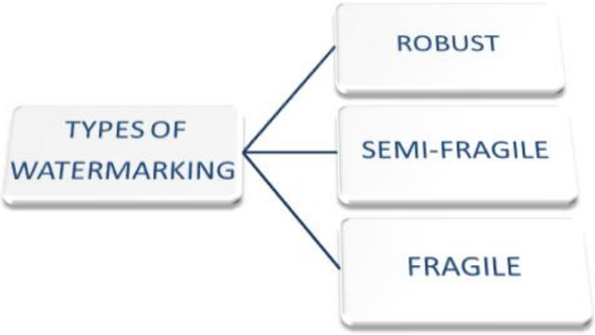
The extracting function (f_x), recovers the embedded watermark on the receiving side. The key used in the embedding process is supposed to be available on the receiving end along with the availability of the original data(informed watermarking) or even without the availability of original data (blind watermarking),

$$W^1 = f_x\ (X, X_w, k) \text{ Or } \ W^1 = f_x\ (X_w, k)$$

Where W^1 is the recovered watermark.

Watermarking can be divided into three broad categories based on the resistance offered by the embedded watermark to various attacks: robust watermarking, fragile watermarking and semi-fragile watermarking.

www.ijcem.in



The robust watermark has the ability to resist the malicious or nonmalicious manipulations. Nonmalicious attacks mainly include processes performed during image processing like JPEG compression, format transformation, quantization, filtering etc. Examples of malicious attacks are cut/copy paste, cloning the image pixels or attempt to mix the pixels with adjacent areas, counter feting, collaging. The main aim of robust watermarking is to resist attacks. It is difficult for robust watermarking techniques to detect the friendly manipulations. So they aren't suitable for communication applications. But it finds its application in other applications. Robustness is application dependent.

Semi-fragile watermarking is a tradeoff between the fragile watermarking and robust watermarking. So, semi-fragile watermarking has the ability to resist the nonmalicious manipulations like JPEG compression and is fragile against the malicious manipulations. The primary application of the semi-fragile watermarking is tamper proofing and authenticating, so the features of the semi-fragile marking system generally resemble those of the fragile watermarking. This type of watermarking finds its applications in communications domains like internet data transfer. These types of techniques are relatively new in the watermarking field. They are not yet complete and still a huge amount of research is going on them. But the results produced by these techniques are most promising and hence many researchers are attracted towards using these techniques and to research on them. To develop enhance performance of these techniques, multiple watermarks are being embedded and techniques which provide authentication and self-restoration properties are also being proposed.

A fragile watermark is a watermark that is readily altered or destroyed when the host image is modified through a linear or non-linear transformation [3]. That is, it may be of interest for parties to verify that an image has not been: edited, damaged, or altered since it was marked. The fragile watermark is intended to be destroyed even after nonmalicious attack. The main application of fragile watermarking is content authentication. The sensitivity of fragile watermarks to modifications leads to their being used in image authentication. Fragile watermarking technique finds its applications where there is a need of high security like military applications, crime investigation.

Based on the domain in which embedding procedure is done is the watermarking techniques are divided into three categories. This classification is shown in the below figure.

www.ijcem.in

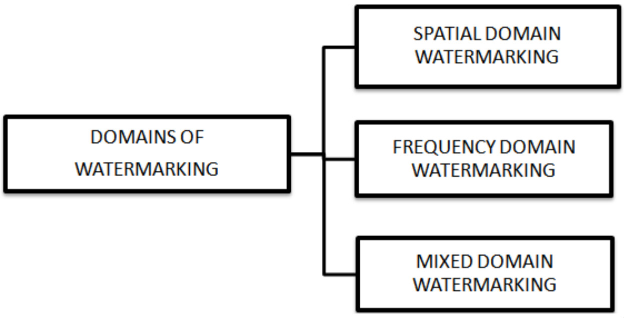

DOMAINS OF WATERMARKING
SPATIAL DOMAIN WATERMARKING
FREQUENCY DOMAIN WATERMARKING
MIXED DOMAIN WATERMARKING

Figure 2: Domains of watermarking

www.ijcem.in

When the watermark is embedded into cover work in the spatial domain the watermarking technique is known as spatial domain watermarking technique. In the spatial domain, pixels in randomly selected regions of the image are modified according to the watermark. This method is as simple as modifying the pixel values of the original image where the watermark should be embedded. Randomly selected image data are dithered by a small amount according to a predefined algorithm which may vary in complexity in practical systems. One of the major disadvantages of the conventional watermarking is that it can be easily extracted from the original image which makes this technique unsuitable for copyright authentication. But the recent experiments have developed many novel spatial domain watermarking methods which overcomes these difficulties and provide better optimization of the three parameters.

The most famous spatial domain watermarking method is LSB substitution technique. This technique involves direct replacement between cover image's LSB and message (watermark) bits by adopting different logical or arithmetic combinations. LSB manipulation programs for a variety of image formats are proposed in the past and are being proposed till date. LSB methods achieve both high payload (high information rate) and low perceptibility. However, because information is hidden in LSB, it is fragile to any data processing, which results in loss of information from these LSB bits. These spatial domain algorithms are appealing because they are simple to calculate, have clear physical meanings, and are mathematically convenient in the context of optimization. But they are not very well matched to the frequency or mixed domain algorithms because perceived visual quality given by SSIM metric for investigating quality of images is low. There are certain drawbacks of such algorithms like low hiding capacity, Low PSNR, original and extracted water marks may not match and so on[10].

The second watermarking techniques which are classified as frequency domain algorithms because all the modifications to the images are done with their spectra. In these techniques the image is transformed into frequency domain representation using any one of the available transformation techniques like DCT, FFT etc. The mostly used transformation technique in case of image processing is DCT (Discrete Cosine Transform). The DCT is the choice of most people because of high image compression capability. And also that it is easier to calculate. DCT eliminates the possibility of complex coefficients for real signals as compared to FFT. The frequency domain representation will consist of the coefficients related image content. The coefficients corresponding to the low frequencies are higher and appear in the up-left corner of the square, while high frequency coefficients appear in down-right with lower absolute values. So if we modify these coefficients the image content is changed. This point is exploited by the frequency domain techniques. The required modifications are done by the frequency domain watermark embedding algorithm. After the required modifications are made the frequency domain representation is converted back to spatial domain representations by performing the appropriate inverse transformation techniques like IDCT etc.

The modifications by the watermarking techniques are made in the mixed domain representation of the image i.e., time-frequency representation. In these type of techniques the image is modified in the both the time and frequency domains. This is possible only if the representation gives the knowledge of both time and frequency at the simultaneously. One of the efficient transformation techniques on this aspect is wavelet transform. This is an emerging tool in the field of image processing. It gained huge amount popularity in image processing domain because it achieves high compression rates. Basically wavelet transform is developed from short term Fourier transform and wavelet means a wave with short time duration. It provides with the information of which band of frequencies are found at which time interval.

In the mixed domain watermarking at first the cover work and the watermark are transformed into time-frequency representation by using discrete wavelet transform. The embedding of watermark is done the mixed domain itself and the resultant image is retransformed into spatial domain by performing inverse discrete wavelet transform.

III. OVERVIEW OF WATERMARKING TECHNIQUES

In this chapter we present an overview of the three techniques that we are going to implement in this paper. As a spatial domain watermarking technique we implement a modified of version of LSB substitution technique. The description of this technique is given in the first section. It is followed by the description of a frequency domain watermarking technique which is based on the famous COX method which uses DCT transforming technique. At last as a mixed domain watermarking technique we implement an algorithm based on wavelet transform.

Spatial Domain Watermarking Technique

In any spatial domain technique the pixel values are directly modified or altered hence they are known as spatial domain techniques. Conventional Spatial domain watermarking is generally not in use due to its least reliability. In the spatial domain, pixels in randomly selected regions of the image are modified according to the watermark desired by the author of the product. This method is as simple as modifying the pixel values of the original image where the watermark should be embedded. One of the major disadvantages of the conventional watermarking is that it can be easily extracted from the original image which makes this technique unsuitable for copyright authentication. In the recent days there are many novel spatial domain techniques proposed which overcome these troubles. the commonly used spatial domain algorithms are Least Significant Bit (LSB) adjustment, Patchwork, Texture Block Coding, etc [4].

The generalized flow of the process followed in the most of the spatial domain watermarking techniques is shown below. Note that all the manipulations are done with the raw pixel data as it is a spatial domain technique representation.

One of the spatial domain techniques which gained much popularity is LSB substitution technique and it is one of the most primitive watermarking techniques. LSB technique is a type of information hiding technique. LSB means the least important bits or the least significant bits. Take a standard Gray level Image for example. Every bit of the image is constituted by the 8-bit binary,

www.ijcem.in

and the essentiality of each bit is different. The highest bit represents the 10000000 in binary while the least significant bit represents the 1 in binary. It reminds that we can embed the watermarking into the least significant bits without destroying the visual sense of the host image.
The traditional LSB algorithm is embedding the watermarking to the least important bits of the host image in sequence. It has huge information capacity, quick embedding speed, and can be hide and extract easily. However, the LSB substitution is simple but it easy for the unauthorized person modify the data.

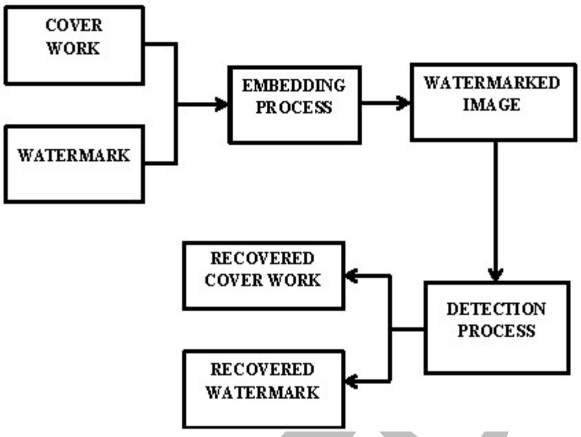


Figure 3: Spatial domain watermarking

In the traditional LSB substitution algorithm, the bits of each pixel were extracted, LSB's were identified and some another information was substituted [5]. This is the basic technique implemented in LSB substitution algorithm. This would require a loop structure to do it and hence execution time of this algorithm is very high.
Instead of this, we can approach this technique in a different way. We can make use of bit-planes. Bit-plane is the plane that one specific bit of every pixel create. The first bit-plane is formed by the least significant bits (LSB) and most of the time is hardly related to the main shapes of the picture. On the other hand, the last bit-plane is formed by the most significant bits (MSB) and contains the main lines and edges of the picture. So we can make use of LSB bit-planes as place to information hiding. This point is being exploited by us in this paper. In our paper we extract bit-planes of the image and hide some information in the non-important LSB bit-planes. This information is related to watermark. The substitution is done using the following equation

WI = 4 msb bit-planes of message + S* (4 msb bit-planes of watermarks)

Here S is the scaling factor which controls the visibility of the watermark in the watermarked image. As the visibility of watermark increases, the performance of watermarking algorithm decreases. After the substitutions are complete the image is reconstructed and the watermarked image is obtained. The receiver also extracts the bit-planes from the received watermarked image and separates the bit-planes. Then the watermark and the cover work are reconstructed by using the appropriate bit-planes to obtain the recovered watermark and the recovered cover work.

Frequency Domain Watermarking Technique

The classic and still most popular domain for image processing is that of the Discrete-Cosine-

www.ijcem.in

Transform, or DCT i.e., frequency domain [6]. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). And the mid-bind scheme is right a tradeoff between the imperceptibility and robustness.

the main advantages of the frequency domain water marking is it is more compatible with JPEG standard. Thus frequency-domain watermarking obtains much more attention. To embed a watermark, a frequency transformation is applied to the cover work. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others.

A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson Cox developed the first frequency-domain watermarking scheme. After that a lot of watermarking algorithms in frequency domain have been proposed. In our paper we make use of 2-dimensional discrete cosine transform (DCT) in the watermarking process. The two images, cover work and watermark which are in spatial domain are converted into frequency domain by using 2-dimensional DCT. The frequency representations are merged into a single DCT by use of the equation

$$WI = C\,(1+s*W)$$

Where WI is DCT of watermarked image, C is DCT of cover work, S is scaling factor, W is DCT of watermark.

Here the scaling factor is used to control the visibility of the watermark in the watermarked image. With the increase in the visibility in the watermark there is an decrease in the performance of the watermarking algorithm. Now the obtained DCT of watermarked image is retransformed into spatial domain by applying inverse DCT.

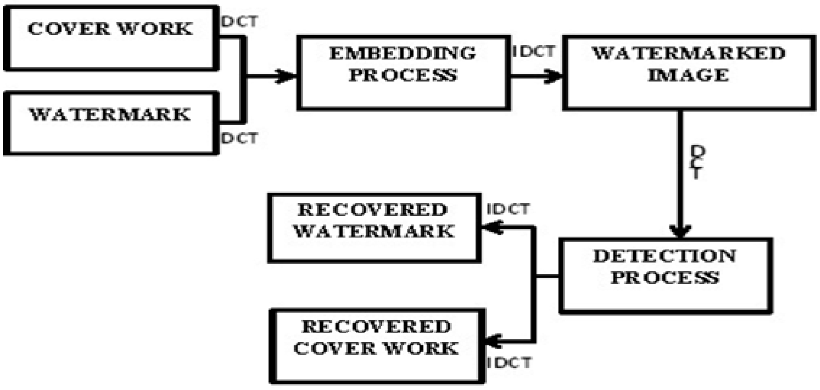


Figure 4: Frequency domain watermarking

Mixed Domain Watermarking Technique

A transparent and robust watermark should be such that the watermark is detectable in the cover work. The proper selection of the frequency transform is dependent on the fact, the better the image transform approximates the properties of the HVS (Human Visual System) the easier is to put more energy in the embedded signal without causing perceptible distortion. According to the

www.ijcem.in

HVS the high frequencies are less visible then the low frequencies. Wavelet transform is more close to the Human Visual System than DCT. DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. The Discrete Wavelet Transform (DWT) is mostly used in various applications like audio and video compression and noise removal in audio[11]. Wavelets have their energy concentrating time and are well suited for the analysis of transient, time-varying signals. since the real time signals are analog in nature so the wavelet transform is used[7].

In this the low frequency signals are located in the frequency domain while high frequency signals are located in the pixel domain. Wavelets have their energy concentrated in time and are well suited for the analysis of the transient, time varying signals. The 2D wavelet transform decomposes an image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The perceptible watermark should be embedded in the low frequency region while the imperceptible watermark should be embedded in the high frequency region.

The new JPEG2000 standard has adopted a new technique, the wavelet transform. Though this standard has not been widely used yet, any new watermarking algorithm that intends to survive in the future should get along with it. Here come the watermarking schemes based on wavelet transform. The difference between different wavelet domain methods depends on the way the watermark is weighted. The reason for this is to reduce the presence of visual artifacts. One of the many advantages over 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 watermarks in these bands will increase the strength of watermark without effecting the quality of the image.

The 2-D discrete wavelet transforms (DWT) decomposes the image into sub-images, 3 details and 1 approximation. The approximation looks just like the original only on 1/4 the scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The slow changing aspects of a signal are preserved in the channel with the low-pass filter and the quickly changing parts are kept in the high-pass filter's channel. Therefore we can embed high-energy watermarks in the regions that human vision is less sensitive to, such as the high-resolution detail bands (LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. The fact that the DWT is a multi-scale analysis can be used to the watermarking algorithm's benefit. Multi resolution is the process of taking a filter's output and putting through another pair of analysis filters. The first approximation will be used as a "seed" image and recursively apply the DWT a second and third time (or however many times it is necessary to perform to find all of the areas of interest).

www.ijcem.in

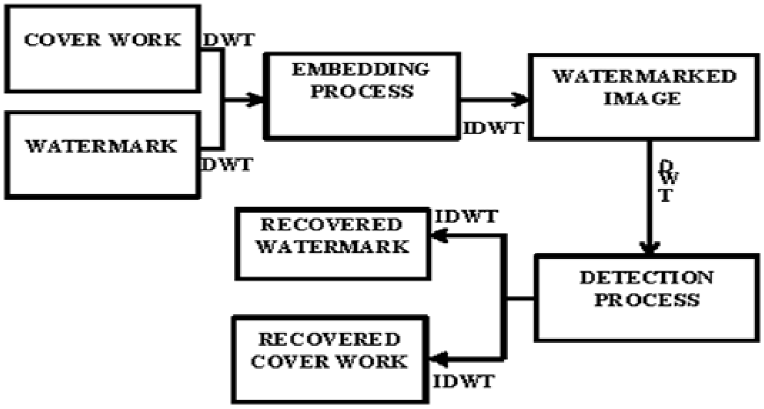


Figure 5: Mixed domain watermarking technique

In our paper we make use of 2–dimensional discrete wavelet transform (DWT) in the watermarking algorithm. The cover work and the watermark are transformed into time-frequency representation by using 2-D DWT. The approximation images of cover work and watermark are blended into single approximation image by use of alpha bending. Alpha bending is described as

$$WI = (k*C) + (q*W)$$

Where WI is watermarked image, k and q are the scaling factors to control the visibility of cover work and watermark, C is the approximation image of cover work, W is the approximation image of the watermark. The constant k is used control the content of the cover work in the watermarked image and as the k value increases the performance of the watermarking techniques increases. Whereas the constant q is used to control the visibility of the watermark in the watermarked image and there is an inverse proportionality between the constant q and the performance of the watermarking technique [8].

IV. IMPLEMENTATION OF WATERMARKING TECHNIQUES

LSB Substitution Watermarking

As a spatial domain watermarking technique, we have implemented a variation of LSB substitution technique. Here we are implementing a variation of the LSB substitution techniques. Instead of dealing with the bits of the each of the pixel, in this technique we deal with the bit-planes formed by the each pixel. The algorithmic description of the technique which we have implemented is given below followed by their matlab implementation.

Transmitter Side Algorithm and Flow-chart

Step 1: Read cover work and watermark images which we are going to use in our technique.
Step 2: Extract their corresponding bit-planes.
Step 3: Substitute 4msb bit planes of watermark into 4lsb bit planes of cover work.
Step 4: Make use of scaling factor to control the visibility of the watermark in the watermarked image.
Step 5: reconstruct the image with the substituted bit planes. The reconstructed image is the watermarked image.
This completes the work which has to be done at the transmitter to generate the watermarked

image. This image is transmitted to the receiver. Now the corresponding matlab implementation is given in the same order.

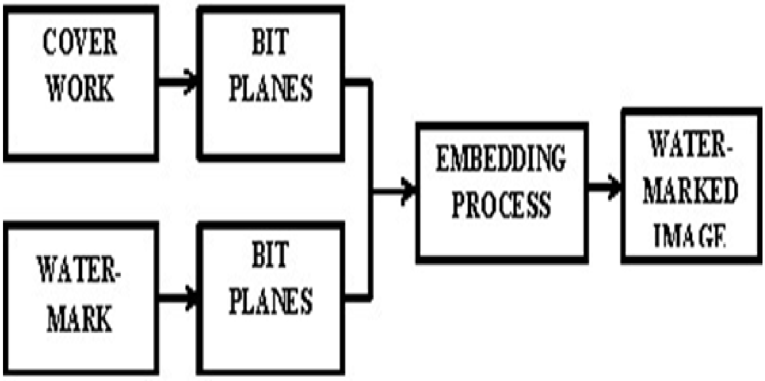


Figure 5: Transmitter side of LSB substitution technique Flow-chart

Receiver Side Algorithm and Flow-chart

At the receiver side, the work which has to be done is given in below algorithm. The receiver extracts the bit-planes of the received image and recovers the cover work and the watermark.
Step 1: extract the bit planes of received watermarked image.
Step 2: reconstruct the recovered watermark by using the 4lsbs bit planes.
Step3: reconstruct the recovered cover work by using the 4msbs bit planes
Step 4: calculate the PSNR and MSE for various values of the scaling factors.
Step 5: state the conclusions based on the visibility of watermark and calculated PSNR.

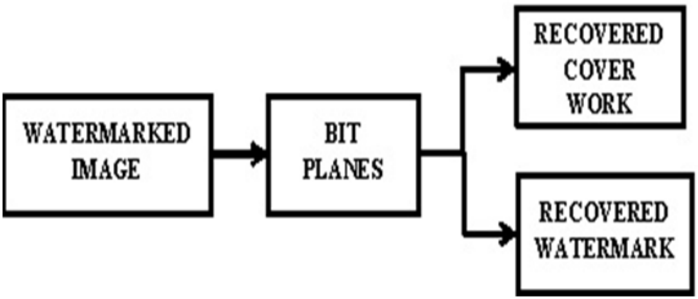


Figure 6: Receiver side of LSB substitution techniques Flow-chart

DCT Watermarking

As a frequency domain watermarking technique, we have implemented a technique based on discrete cosine transform (DCT). In this technique the images are transformed into frequency domain using DCT, and then the watermark is embedded into the cover work. As it is a frequency domain technique all the manipulations are done in the frequency domain itself.

Transmitter Side Algorithm and Flow-chart

Step 1: read the cover work and the watermark
Step 2: perform DCT on both the images to transform them into frequency domain
Step 3: assume a scaling factor to control the visibility of the watermark in watermarked image
Step 4: modify the DCT of cover work using DCT of watermark and the scaling factor using the

www.ijcem.in

equation
WI = C + (1+S*W)
C: DCT of cover work
S: scaling factor
W: DCT of watermark
WI: DCT of the watermarked image
Step 5: perform inverse DCT on the constructed DCT of watermarked image to get the watermarked image.

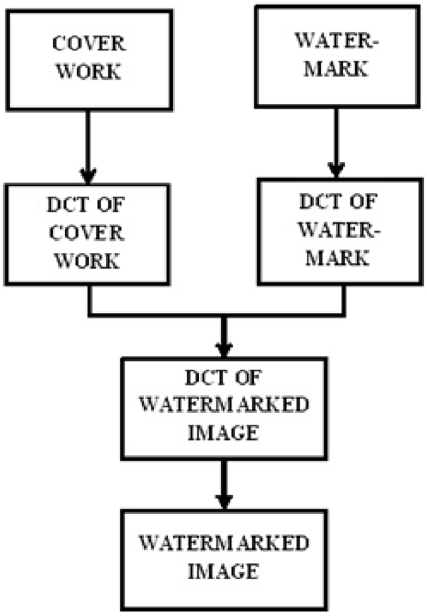


Figure 7: Transmitter side of DCT watermarking technique Flow-chart

Receiver Side Algorithm and Flow-chart
Step 1: perform DCT of the received watermarked image

Step 2: extract the DCT of the watermark to recover watermark using the equation
WR = (1/S)*(WI-C)-1
WR: DCT of recovered watermark
WI: DCT of received watermarked image
C: DCT of cover work
S: scaling factor

Step 3: perform inverse DCT of the extracted DCT of the watermark to get recovered watermark image

Step 4: calculate PSNR and MSE of the recovered watermark.

Step 5: make the required conclusions based on the various values of the scaling factor.

www.ijcem.in

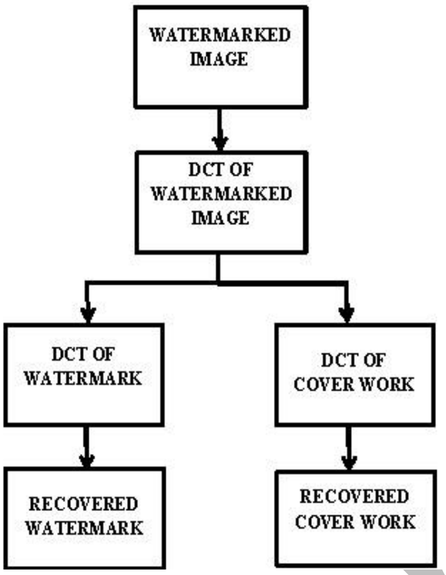


Figure 8: Receiver side of DCT watermarking technique

DWT Watermarking

To implement a mixed domain watermarking technique, we have implemented a technique based on discrete wavelet transform (DWT). In this technique the images are transformed into mixed (time-frequency) domain using DWT, and then the watermark is embedded into the cover work. As it is a mixed domain technique all the manipulations are done in the mixed domain itself.

Transmitter Side Algorithm and Flow-chart

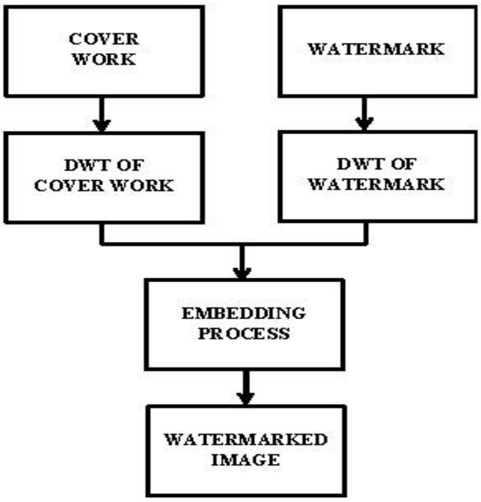


Figure 9: Transmitter side of DWT watermarking technique

Step 1: read the cover work and watermark

Step 2: perform 2 level dwt of both the images

www.ijcel.in

Step 3: choose two scaling factors k and q to control visibility of cover work and watermark respectively

Step 4: embed the watermark into cover work using the equation of alpha bending given as
WI=(k*Ca)+(q*Wa)
WI: watermarked image
k: constant to control content of cover work
q: constant to control visibility of watermark
Ca: approximation image of cover work
Wa: approximation image of watermark

Step 5: the result of alpha bending is watermarked image@ubheading should be 10pt Times new Roman, justified.

Receiver Side Algorithm and Flow-chart
Step 1: perform idwt of the received watermarked image

Step 2: extract the watermark using the equation
WR= WI - k*Ca
WR: recovered watermark and WI: watermarked image
k: constant to control content of cover work
Ca: approximation image of cover work

Step 3: extract the cover work using the equation
CR = WId -(q*Wa)
CR: recovered cover work
WId: DWT of the watermarked image
q: constant to control visibility of watermark
Wa: approximation image of watermark

Step 4: calculate the PSNR and MSE.

Step 5: make the required conclusions based on the observations made for different values of the constants k and q.

www.ijcem.in

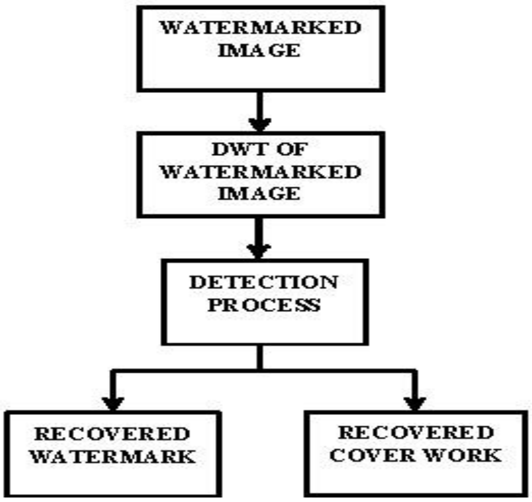


Figure 10: Receiver side of DWT watermarking technique

V. PERFORMANCE EVALUATION TOOLS

The performance of the watermarking techniques can be evaluated by calculating the various specifications. In this paper we calculate MSE (mean squared error) and PSNR (peak signal to noise ratio) of the recovered watermark and the original watermark to evaluate the performance of the three techniques developed. To calculate these values we have written a user-defined function. The dependence of the performance of watermarking technique on these values can be found in the next chapter.

Mean Squared Error (MSE)

The MSE compares the two input images and finds the error at each pixel by subtraction and finds the mean square of the resultant error. So in the developed code we supply the recovered watermark and the original watermark as the two input images. So the MSE calculates the difference at each pixel and the result of this difference is the error between the two images. To better represent the error we square the error and find its mean. This is the resultant MSE. This is given by following equation.

M.S.E=1/n* (X1-X2) 2

Where X1 and X2 are two input images

Peak Signal to Noise Ratio

Pick Signal to Noise Ratio (PSNR) is a better test since it takes the signal strength into consideration (not only the error).

$$PSNR=10*\log_{10} (MAX_1/MSE)$$

Where MAX_1 is the maximum signal power in the first input image and MSE is mean squared error of the two images.

The performance of the watermarking technique is evaluated by PSNR as the value of the PSNR is high the performance is high. Hence there is a direct relationship between the performance of the watermarking technique and the value of PSNR.

www.ijcem.in

VI. EXPERIMENTAL RESULTS

In this chapter we present you with results of the three watermarking techniques which we have developed. This chapter evaluates the performance the three watermarking techniques based on the values of MSE and PSNR included in the tabular columns. With the tables consisting of these values we can theoretically draw conclusions about the dependence of performance of the watermarking technique. And with images included we can visually confirm the conclusions drawn theoretically.

We have used the same cover work image and watermark image as inputs to all the three techniques for better and exact evaluation. As the same images are used it is easy to compare the techniques visually. The cover work image which we are using is the famous image of cameraman and watermark image used here is pout image. They are shown in the below figure.

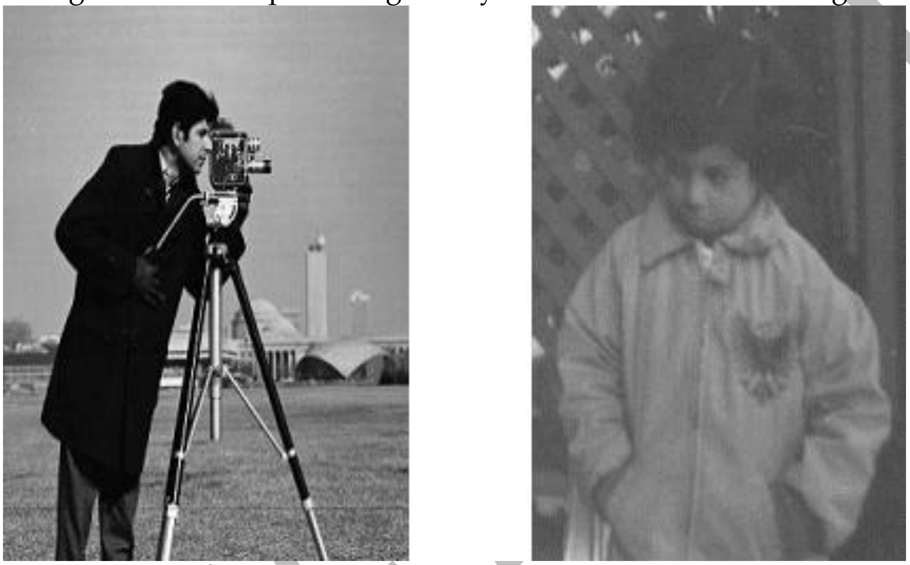
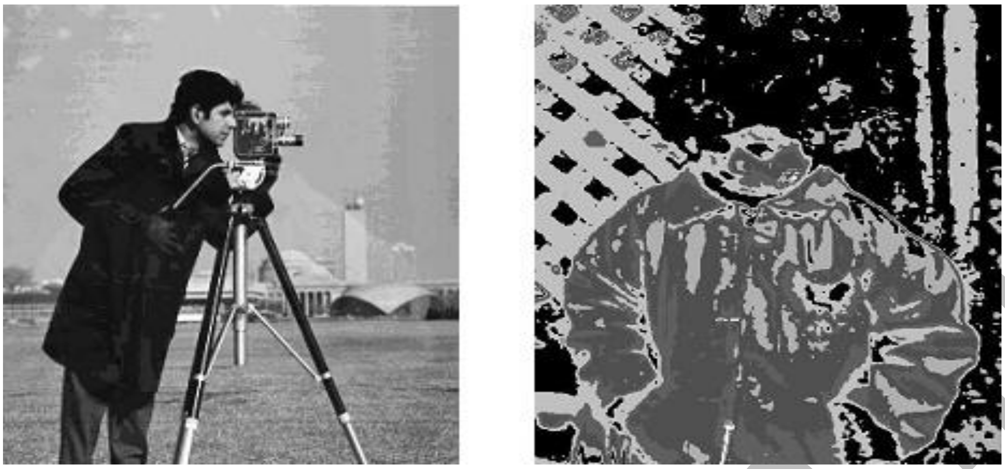


Figure 11: Cover work and watermark

LSB substitution watermarking

As the LSB substitution technique is the most primitive technique, we could least expect the better performance from it. As the images shown in the next figure the watermark isn't recovered successfully because the signal content of the watermark is low in the watermarked image. The reason for the low content in watermarked image is that the substitution of the MSB's into LSB's of the cover work by which the watermark image content is suppressed.



a) Watermarked image *b) recovered watermark*

Figure 12: Results of LSB technique for s = 0.5

The images shown below are the best possible images resultant for the scaling factor value of s=0.5. In the below figure, the image showing the cameraman is the watermarked image for the scaling factor of s=0.5. The image besides it is the recovered watermark image of pout extracted from the watermarked image. The LSB substitution technique doesn't allow the freedom to choice of wide range of the scaling factor values. Hence we can't freely control the visibility of the watermark. This is an added disadvantage of this technique.

Table 1: Readings of LSB substitution technique

S (scaling factor)	MSE	PSNR
0.01	154.1134	46.6637
0.1	97.1678	60.9864
0.2	83.6160	65.3504
0.5	4.4704	94.6379

The performance tools calculated for various values of scaling factor are tabulated in the above table. As observed the MSE and PSNR values are indicating a poor performance of the technique. As the scaling factor increases, the visibility of watermark increases i.e., the content of the watermark increases. This will reduce the value of MSE and increase the value of PSNR. The readings are matching the above stated assumptions.

DCT watermarking

The DCT based watermarking technique offers better performance than LSB substitution technique. And also it provides choice of wide range of values for scaling factor. Hence the visibility of the watermark is control efficiently and it can be seen in the following figures.

In the above figure, the watermarked images for various values of scaling factors are shown. The

www.ijcem.in

orders of images are shown follows decreasing value of the scaling factor. The observation to be made here is the visibility of the watermark is decreasing as the value of the scaling factor is decreasing. The decreasing scaling factor results in the increase in the MSE and decrease in the PSNR. So we must make a trade-off between the visibility of watermark and performance of the technique. This trade-off is application dependent. If the extreme cases of the above images are considered that are images with s=1 and s=0.01. The watermarked image with s=1 has significant visibility of the watermark and it can be considered as the visible watermarking. On the other extreme the watermarked image with s=0.01 there is no visibility of the watermark and it can be considered as invisible watermarking.

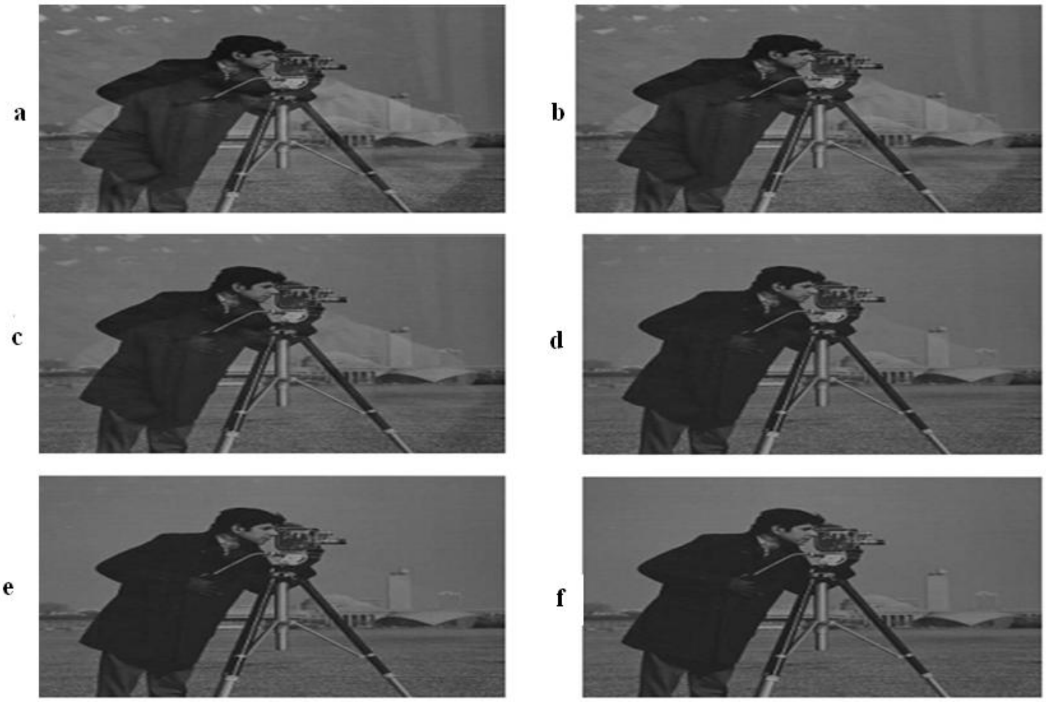


Figure 13: Watermarked Images of DCT based technique for various s values
a) for s=1 b) for s=0.75 c) for s=0.5
d) for s=0.2 e) for s=0.1 f) for s=0.01

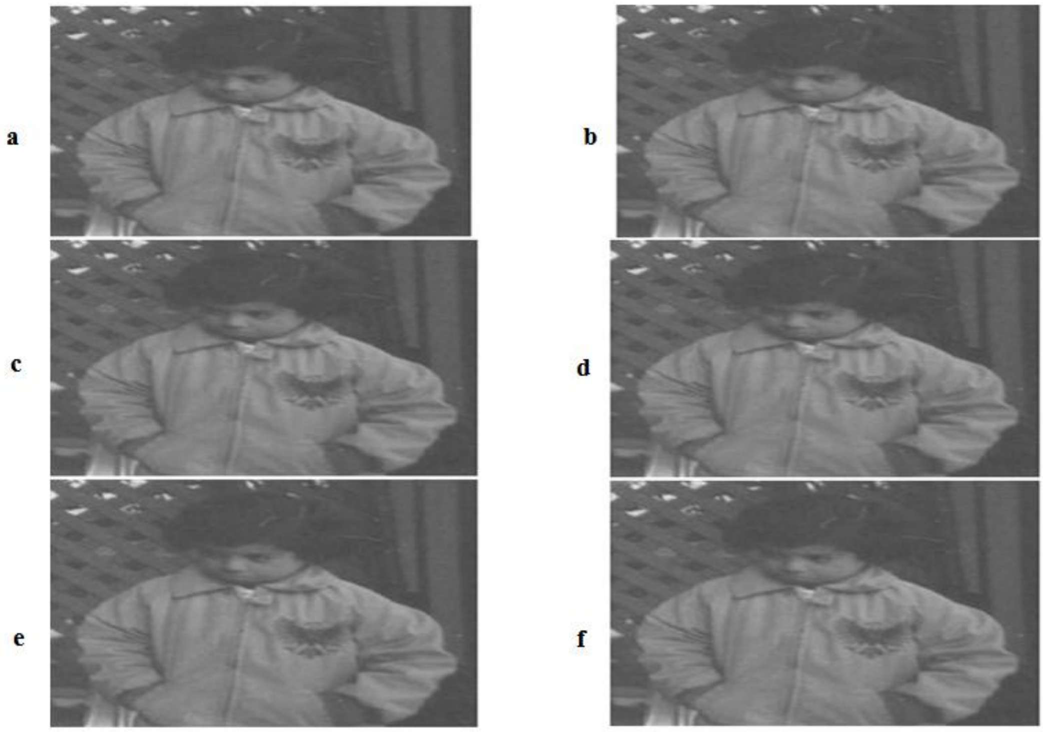


Figure 14: Recovered watermarked Images of DCT based technique for various s values
a) for s=1 b) for s=0.75 c) for s=0.5
d) for s=0.2 e) for s=0.1 f) for s=0.01

The tabulated values below are proving the concept that the parameters visibility of the watermark and performance of watermarking technique contradict. As observed upon decrease in the value of the scaling factor results in the invisible watermarking but at a cost of low performance as shown by the MSE and PSNR values. So as mentioned earlier, there must be a trade-off between the visibility and the performance.

Table 2: Readings of DCT based technique

S (scaling factor)	MSE	PSNR
0.01	3.3901	158.1428
0.1	0.4282	166.6745
0.2	0.1809	173.5878
0.5	0.0371	200.3376
1.0	0	Inf

www.ijc

DWT watermarking

As the improvement to the previous techniques it offers better performance than the other two techniques. It also offers a choice of choosing scaling factors from a very wide range of values. The values shown in the below table are obtained for a value of k lower than q. It is observed that for any value k value greater than or equal to q gives zero MSE and infinite PSNR. So it depicts that the performance of the wavelet based technique is the best offered performance in all the three techniques.

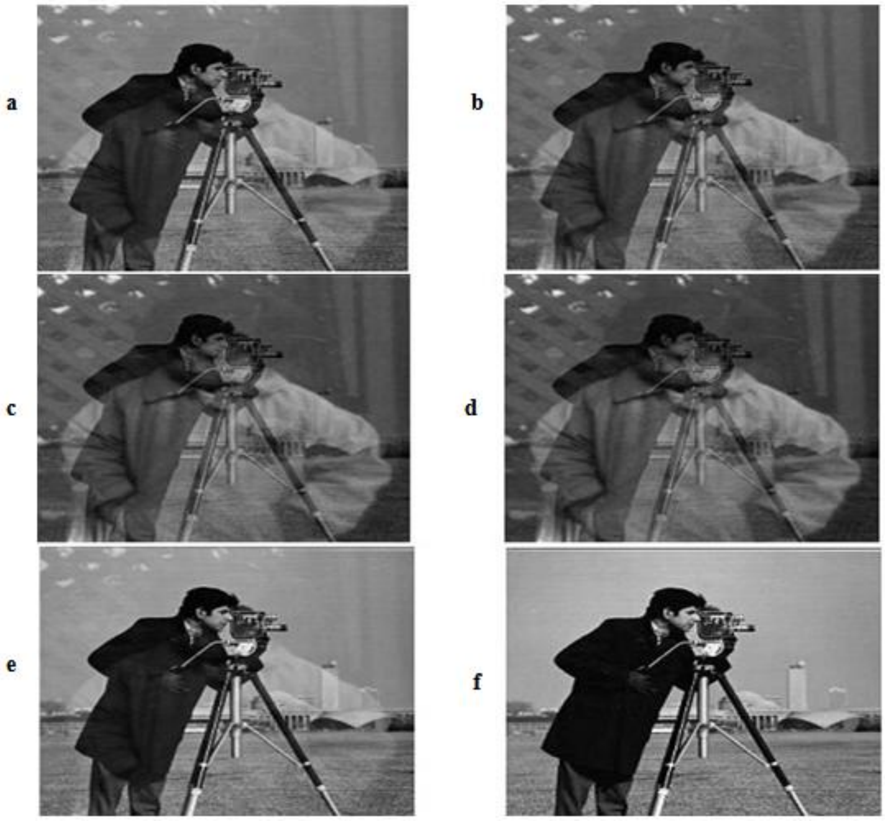


Figure 15: Watermarked images of DWT based techniques for various values of k and q
a) for k=0.1&q=0.1 b)for k=0.1&q=0.2 c)for k=0.1&q=0.3
d)for k=0.1&q=0.4 e)for k=0.2&q=0.1 f)for k=0.5&q=0.005

The figure shown above consists of the watermarked images for various values of k and q. The constant k controls the content of the cover work whereas the constant q controls the visibility of the watermark.

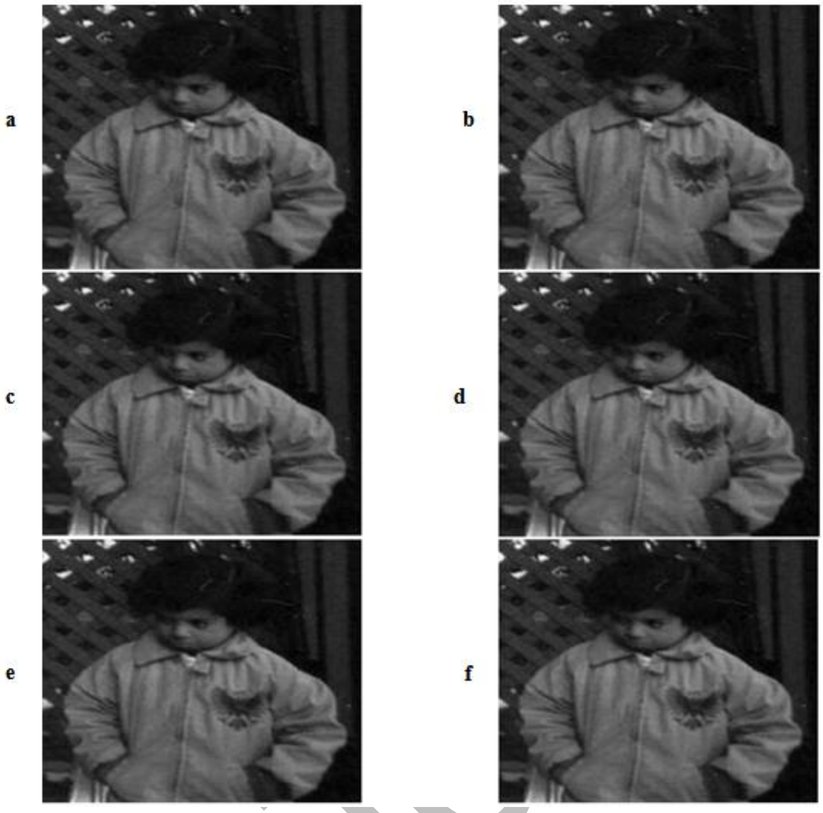


Figure 16: Recovered watermark images of DWT technique for various values of k and q
a) for k=0.1&q=0.1 b)for k=0.1&q=0.2 c)for k=0.1&q=0.3
d)for k=0.1&q=0.4 e)for k=0.2&q=0.1 f)for k=0.5&q=0.005

The figure shown above consists of the recovered watermark images for various values of k and q. As seen that the quality of all the recovered images is far better than the quality provided by other two techniques

As the table suggests the MSE value is zero in most of the cases and with infinite PSNR value showing the better performance of the DWT based watermarking technique. The reading shown for k=0.1 and q=0.4 is the worst case performance of this technique which is far better than the other two techniques. As the value of the constant q increases the performance decreases and increase in the value of k increases the performance.

Table 3: Readings of DWT based technique

K	Q	MSE	PSNR
0.1	0.1	0	Inf
0.1	0.2	0	Inf
0.1	0.3	2.9805	68.3057
0.1	0.4	36.0970	87.4934

www.ijcem.in

0.2	0.1	0	Inf
0.5	0.05	0	Inf

VII. CONCLUSION

In this paper, three watermarking techniques are developed one from each domain. The techniques developed are newest and simple in their respective domains. So we can compare the advantages and disadvantages of each technique and we can choose the appropriate watermarking technique which suits for our application. The choice is better made when we consider the performance evaluation tools. A user can make a choice from the three techniques offered and he can come to a conclusion based on the MSE and PSNR values provided. Hence the importance of this paper is that it develops three new watermarking techniques, evaluates each of them and also provides a choice to the user to choose best technique.

REFERENCES

[1] Swanson, Mitchell D., Mei Kobayashi, and Ahmed H. Tewfik. "Multimedia data-embedding and watermarking technologies." Proceedings of the IEEE 86.6 (1998): 1064-1087.

[2] Boyle, Roger D., and Hazem Hiary. "Watermark location via back-lighting and recto removal." International journal on document analysis and recognition 12.1 (2009): 33-46.

[3] Raja'S, Alomari, and Ahmed Al Jaber. "A fragile watermarking algorithm for content authentication." International Journal of Computing & Information Sciences 2.1 (2004): 27-37.

[4] Podilchuk, Christine I., and Edward J. Delp. "Digital watermarking: algorithms and applications." IEEE signal processing Magazine 18.4 (2001): 33-46.

[5] Swanson, Mitchell D., Mei Kobayashi, and Ahmed H. Tewfik. "Multimedia data-embedding and watermarking technologies." Proceedings of the IEEE 86.6 (1998): 1064-1087.

[6] Zain, Jasni Mohamad, and Malcolm Clarke. "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images." arXiv preprint arXiv:1101.1603 (2011).

[7] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on. IEEE, 2005.

[8] Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." Proceedings of the IEEE 87.7 (1999): 1062-1078.

[9] Lakshman, J. I., and Smeer Awasthi. "Relative Analysis of Indiscernible Text Digital Watermarking."

[10] Gunjal, Baisa L., and Suresh N. Mali. "Insight into New Color Image Watermarking With DWT-DCT and only DCT with Comparative Analysis in YIQ Color Space."

[11] International Journal of Advanced Research in Computer Science 3.3 (2012). Pithiya, Pravin M., and H. L. Desai. "DWT Based Digital Image Watermarking, De-Watermarking & Authentication." image 1.2 (2013): 7.

www.ijcem.in