# ROBUST DIGITAL WATERMARKING TECHNIQUE AND PROCESS FOR DIGITAL CONTENT AND IMAGE COPYRIGHT PROTECTION

**LAKSHMAN JI [*1], GOPAL PATIL[*2] , Dr. SHIV KUMAR**

**PhD research scholar**

**Department of Computer Science and Engineering**
**SARVEPALLI RADHAKRISHANAN UNIVERSITY,BHOPAL**
**Hoshangabad Rd, Near Nissan Motors, Misrod, Bhopal, Madhya Pradesh 462026**

**Abstract:-** This paper presents a thorough literature review of robust digital image watermarking applied in diverse applications. Researchers have already done lots of noteworthy work in the field of digital image watermarking. Even though, it is interesting to point out that current methods designed for image integrity may not be perfect. Therefore, the main aim of this paper is to offer a comprehensive reference source to the researchers involved in the design of robust digital image watermarking schemes, regardless of particular application areas The arrival of digital world coming soon, the digital media content can be easily altered, duplicated, and spread, which causes the copyright of media are violated. Therefore, attention is to discuss the protection of the intellectual property (IP) rights of digital media.audio video images Text Then, the digital watermarking can be a simple and effective approach to provide copyright protection of IP. In this study, a method of robustness and blind

**Keywords** Copyright protection Text image and audio video documents for Digital Watermarking , Image registration watermark DCT Copyright protection **.**

**Author name -LAKSHMAN JI**
**EMAIL- lkshmanji@gmail.com**

## Introduction

Komatsu and Tominaga first proposed the term of the digital watermark in 1988 The technique of the digital watermark had more studies and applications fields till 1990 The major purpose of the digital watermark is to effectively provide the copyright protection of intellectual property, digital content which is thoroughly protected by law to ensure that the rights of original authors are not violated Then, the structure of the watermark and extraction and verification is shown in Fig. 2. The operation of watermark extraction can be gotten from the original image, embedded image,

The sophisticated developments in the technology provide high quality processing capabilities, flexibility, and reliability at lower costs when compared with the analog systems. As a result, digital image acquisition, processing, storage and reproduction systems are gradually replacing their analog versions. Nevertheless, the declining technological barriers, i.e. lack of built-in integrity and quality verification mechanisms, have emerged as the greatest threat

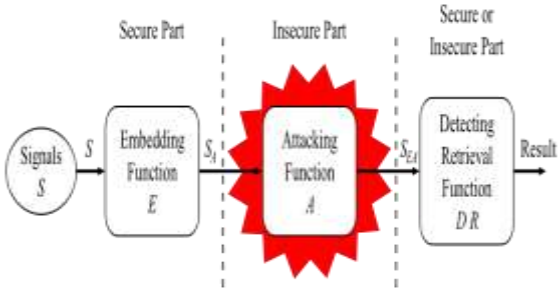



**Image Integrity Protection-** Traditionally, due to the limited processing abilities in analog media, malicious manipulation of images has been a tedious task with only inferior results being realized without prohibitively expensive professional equipment. However, digital images, unlike their analog versions, can be easily maneuvered using a variety of intricate signal processing tools that are easily

available as commercial packages. Photo-realistic tampering can be done by almost everyone using low-cost hardware and software components. The ease and extent of such tweaking raise serious disputes about the integrity and authenticity of digital images. Potential security loopholes of shared information networks, e.g. Internet, on which digital images are commonly posted and distributed further exacerbates the problem. As a result, in applications, where verification of integrity and authenticity of the image content is essential, there is a need for secure image authentication techniques. Multimedia authentication techniques are usually designed either using digital signature or watermarking. A digital signature is a data string which associates a message with some originating entity to simulate the security properties of a handwritten signature on paper. Digital signature technique is a section of cryptography, and is based on algorithms like RSA, DSA encrypted version of the message digest extracted from the data and is usually stored in a separate file, which can be attached to the data to prove integrity and ingenuity. Normally, digital signature schemes (figure 1-1) provide two algorithms, one for signing which involves the user's secret or private key, and one for verifying signatures which involves the user's public key. Conceptually, the hash of data to be transmitted is generated along with originator information and is encrypted and stored in a separate file called “digital signature”. The receiver gets both the data and the signature file. The signature is decrypted at the receiver end and the hash is compared with the received data. If both match, the received data is treated as authentic.

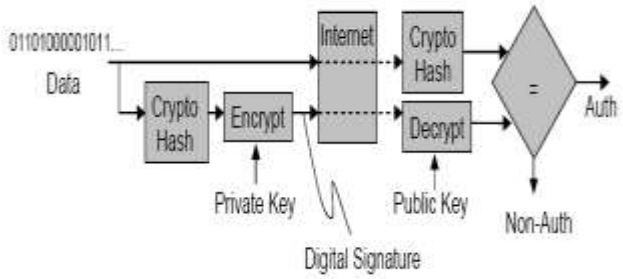
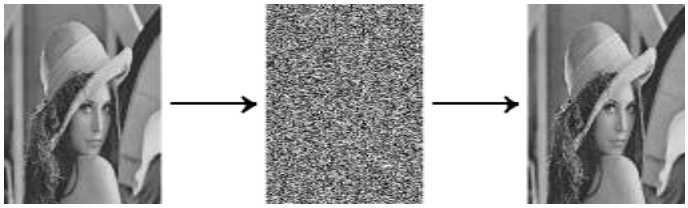



Figure 0-1: Authentication and verification using digital signatures

**LITERATURE SURVEY**

The different audio and video image text documentes hybrid watermarking techniques are studied for checking the robustness. These techniques are very means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper



**Digital Watermarking**

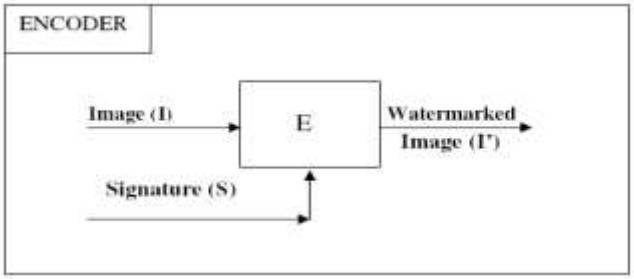
Unlimited number of replicas of the original content can be made from unprotected digital content. This makes the content creators and content owners more concerned about the copyrights management of their digital contents. Apprehensions for the protection of copyrighted digital intellectual properties have been high, since 1980s. The cryptographic algorithms can resolve many of these issues. However, these solutions can only protect the digital contents if they never leave the digital domain and till the content is not decrypted. Once content is decrypted and copied, there is no protection offered. This situation calls for technological solutions to be used in addition to the cryptography technology. Digital Watermarking technologies, a descendent of steganography, have evolved as a major solution for the resolution. This group of technologies provides methods to “imprint” additional data or messages into multi-media contents such as still image, video and audio data. Generally, the imprinted data is invisible (or inaudible) to the ordinary users, and is difficult to be separated from the host media. The imprinted data can be extracted, but not

removed, from the imprinted host media by the legitimate owner, as and when required.

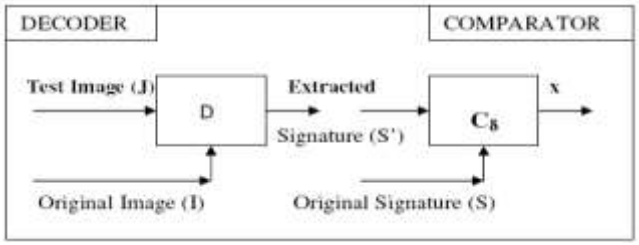
Figure 0-1: Figure showing visible watermarking

## Basic Watermarking Principles

All watermarking methods share the same building blocks: a watermark embedding system and a watermark recovery system and/ or a comparison system. Figure 1-6 below shows the generic watermark embedding process. The input to the scheme is the watermark (or signature), the image (or cover data) and an optional key. The key is used to enforce security, which is preserving unauthorized parties from recovering and manipulating the watermark. The output of the watermarking scheme is the watermarked data.




The generic watermark recovery process is depicted in figure 1-7. Inputs to the scheme are the test image data, the original image data and the optional key. The output is the recovered watermark, if the test image data is watermarked and is an authentic one. The recovered watermark is subjected to the comparator to verify the authenticity of the watermark embedded**.**




## General Digital Watermarking Methods

This section outlines general digital watermarking methods for text, images, audio and video data. These medium differ in ways that present unique problems for watermarking. Still the principle of watermarking remains the same.

**Image**: Watermarking of images typically modify pixel intensities or transform coefficients. An image may be subjected to a great deal of manipulation such as filtering, cropping, geometric transformations, and lossy compression etc. Thus imperceptibility, robustness are usually the most important properties of image watermarks. One of the plausible hardships in image watermarking is the availability of finite bandwidth, thus, as the image size decreases, the permissible watermark length decreases.

**Audio:** As in images, the watermarking desirable characteristics for audio data are imperceptibility, watermark bit rate, robustness, security, and computational cost. Audio watermarking uses the time and frequency masking properties of the human ear to conceal the watermark, and make it inaudible. One of the techniques for audio watermarking is by hiding short echoes, of size a few milliseconds, that can't be perceived by human auditory system. One of the plausible hardships is the need to keep the watermark even after a certain number of re-encoding and digital-analog-digital transfer processes.

**Video:** Digital video is a sequence of still images, and many image watermarking techniques, those can be implemented in real-time, can be extended to video. In contrast to single images, the large video bandwidth means that long messages can be embedded in video. Speedy embedding and extraction to watermark is one of the key issues because of the huge amount of data that must be processed. Beyond those for still image compression, video watermarking poses some unique requirements like frame shuffling, inter-frame collusion, etc.

**Text Document:** Watermarking raw texts are very difficult because of the difficulty to define the appropriate place in which to embed hidden information. Brassil et. al., (1999 July) have

investigated text watermarking and proposed a variety of methods for embedding hidden messages in PostScript documents. They exploited layout information of the text like word spacing, line spacing, text formatting etc. One of the major challenges is that optical character recognition (OCR) can remove any layout information but OCR is expensive, imperfect and often requires manual supervision.

**Characteristics of watermarking systems**

It is essential to define the criteria of a watermarking system for the comparison results against equivalence of group of the assessment attained by assessing the performance of other watermarking methods. Obviously, each watermarking system should have particular properties regarding the given application; therefore, there is no unique set of properties that all watermarking systems have to satisfy. Generally, there are five important issues that are

***1 Imperceptibility***

Imperceptibility is an essential condition for digital watermarking; that is, the visual similarity between the watermarked version and original one of the media element and the perceptual quality of the original signal should be transformed imperceptibly by the insertion of the watermark. There are two main reasons why it is important to keep the imperceptibility of the host media after the encoding with watermark data. Firstly, the presence or absence of a watermark cannot be distinguished from the primary purpose of the original media, if the watermarked media is so badly distorted that its value is lost. In addition, suspicious perceptible artifacts may introduce a watermark in existence, and perhaps its precise location being detected from host media. This information may provide accesses for distorting, substituting, or removing the watermark data maliciously. Therefore, the information embedded in it may no longer be available.

*2 Robustness*

One of the most commonly measured properties is that watermark signals must be reasonably resilient to various attacks and common signal processing operations in digital watermarking systems. Once some watermark signal is inserted in the original content, distortions may be applied to the signal unavoidably when the signal is encoded, decoded, and distributed across the Internet. These distortions may be designed to apply the expected distortion to the watermarked signals or compress it before transmission, and they may or may not significantly disrupt the watermarked signals. It is impossible for a watermarking system to be robust against all signal processing operations whereas the requirement is application subordinate and dependent. For the digital watermarking of images, the good watermarking method is likely to resist against noise addition, filtering processing, geometrical transformations such as scaling, translation and rotation, and also JPEG compression.

*4.3 Capacity*

Capacity is defined using the largest quantity of information that inserted watermarks are capable of hiding, and embedded watermarks can be extracted credibly for the purposes of authentication, and copyright safeguards. Under the condition of imperceptibility as well as the requirements of robustness, the capacity relies on the size of the original data. The more original patterns are attainable, more bits are able to be embedded. However, inserting as much watermark information as possible is a more difficult task in digital watermarking. Very often, a prerequisite for capacity relies on the practicable application used for watermarking. For the audio, the capacity would relate to the amount of inserted bits in every second that is communicated. For images, the capacity may refer to the amount of embedded bits into pixels or patterns of the images. For the video, the capacity refers to either the amount of bits in every second or the bits' amount per frame. In a word, the fewer the amount of bits of capacity included in a watermark, the larger the opportunity of it being computationally complex; fewer false positives or finer granularities and bigger capacity will enlarge the potential operations of the data inserting method and construct the verification judgment more credible. Note: Therefore, the conditions of imperceptibility, robustness, and capability are conflicted and limited by each other. One may want to increase the watermarking strength in order to increase the robustness but these results in a more perceptible watermark. On the other hand, under the condition of imperceptibility, a watermark would have to be created with the maximum possible separation to avoid a

situation where a small corruption of the watermarked image would lead to erroneous watermark detection. Similarly, one can increase the data payload by decreasing the number of samples allocated to each hidden bit but this is counterbalanced by a loss of robustness. In other words, for any watermarking scheme, it is impossible to meet these three requirements simultaneously. As a result, a good trade-off among these requirements has to be achieved.

*4.4 Security*

All existing watermarking algorithms which are not secure cannot be used for copyright protection, data authentication, or tracking the illegal distribution of digital content Therefore, the watermarking algorithm is safe and robust, if the attacker, using watermarking procedures and knowledge, does not know the key used for watermarking digital content. Thus, the hidden watermark information cannot be destroyed or damaged. In addition, the complexity of the watermark process may be safety- related because the attacker will be discouraged to search the insertion in an embedding space and long key position. Therefore, in order to improve the security of the algorithm, it can enlarge the embedded space, and increase the size of the keys split into small pieces of cover image.

***4.5 False positive***

A false positive is defined as not actually containing the watermark in the process of watermark detection. It refers to the amount of false positives that it is predictable to happen in a precondition amount of runs of the detector. Likewise, the possibility can be discussed about any precondition detector run by a false positive occurring. There are two subtle distinctive ways to describe this probability, which are often confusing in some papers. The two diverge in whether the host image or the watermark is contemplated the arbitrary variable. In the first explanation, the false positive probability is the possibility that precondition a settled host image and arbitrarily chosen watermarks, the detector will state that a watermark exists in that image. The watermarks are constructed from a perturbation that is defined by the design method of a watermark construction. Conventionally, watermarks are generated either by a Gaussian sequence or by a bit-encoding algorithmic rule, unrelated to random number generating systems. In common situations, the false positive probability, depending on this first definition, is truthfully sovereign of the host image and only rely on the approach of generating a watermark. In the second definition, the false positive possibility is that randomly chosen images and preconditioned a settled watermark. The detector will retrieve that watermark in an image. The perturbation is greatly application-based determined, where the image is chosen. Medical images, natural images, music videos, graphics, and surveillance video all possess very distinctive statistics. Moreover, while these perturbations are varied from each other, also they are probable to be specific varied from the statistics method of the watermark generation systems. Hence, this second definition of false positive probabilities is absolutely distinctive from the first definition of them.

**Classification of digital watermarking**

**Digital Watermarking for Copyright Protection**

Copyright protection appears to be one of the first applications for which digital watermarking were targeted. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. If users of digital content (music, images, and video) have easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content. An example of one commercial application created for that purpose is Digimarc Corporation's ImageBridge Solution. The ImageBridge watermark detector is made available in a form of plug-ins for many popular image processing solutions such as Adobe PhotoShop or Corel PhotoPaint. When a user opens an image using a Digimark-enabled application, Digimarc's watermark detector will recognize a watermark. It will then contact a remote database using the watermark as a key to find a copyright owner and his contact information. An honest user can use that information to contact the copyright owner to request permission to use the image.

**5.2 Fingerprinting**

Additional data embedded by watermark in this application is used to trace the originator or recipients of a particular copy of multimedia file. For example, watermarks carrying different serial or ID numbers are embedded in different

copies of multimedia information before distributing them to a large number of recipients. The algorithms implemented in fingerprinting applications need to be invisible and must also be invulnerable to intentional attacks and signal processing modifications such as lossy compression or filtering. Fingerprinting should be resistant to the collusion attack, that is, it is impossible to embed more than one ID number in the host multimedia file; otherwise, a group of users with the same image containing different fingerprints would be able to collude and validate the fingerprint or create a copy without any fingerprint.

**3Copy Control**

Watermarks can also be used for copy prevention and control. Fragile watermarks can be used for copy control by having digital player devices detect a fragile watermark and refuse to play a music file or a video clip if no proper signature watermark is detected, preventing people from making illegal copies of copyrighted material. The main challenge that such systems face is that the whole system will only work if all player devices contain a watermark detector. Users will always choose a device that can play and record illegal copies. Actually, a copy protection mechanism that includes digital watermarking at its core is currently being considered for standardization and second generation DVD players may well include the ability to read watermarks and act based on their presence or absence

The above represent a few example applications where digital watermarks could potentially be of use. In addition, there are many other applications for rights management and protection like tracking use of content, binding content to specific players, automatic billing for viewing content, broadcast monitoring, among others. From the variety of potential applications exemplified above, it is clear that a digital watermarking technique needs to satisfy a number of requirements. Since the specific requirements vary with the application, watermarking techniques need to be designed within the context of the entire system in which they are to be employed. Each application imposes different requirements and would require different types of invisible or visible watermarking schemes or a combination thereof.

**6. Attack operators**

The assessment of watermarking systems supplies an automated and fair analysis of substantial watermarking methods for chosen application areas. At present, numerous investigators and researchers utilize their own designed assessment systems, which does not require the capability of comparison each other. Therefore, The assessment procedure can be very complicated, and the current research is on assessment methods with unique attacks for images (for example, attainable tools

***6.1 Removal attacks***

Removal attacks intent to accomplished removing watermarks from the host image. This classification includes lossy compression, denoising, demodulation, quantization, averaging and collusion attacks.

***6*.1.1 Denoising and lossy compression attacks**

This category of attacks is relatively broad and contains common image processing operators such as lossy compression, image denoising and quantization. Image denoising, also understood as filtering, is mainly related to maximum likelihood, a minimax criterion or a minimum mean square error, a maximum a posteriori probability. The resulting filtering operator is decided by the selected criteria, and also by the priors on the cover image and the watermark. Compression is a popular scheme for attacking watermarked images or audio. Two common compression schemes: lossy compression, such as VQ compression, and JPEG compression for image processing have lately been considered to have approximately the same impact on noise removal as denoising. For the attackers to remove the hidden watermarks, they may compress the watermarked images with some other VQ codebooks and decode the VQ indices to get the reconstruction. The VQ compression schemes are effective for attacking some of the existing algorithms. Both lossy compression and denoising can importantly diminish the capacity of the watermarking channel establishing the output of various substitutable channels to zero for each bit of watermark.

**6.1.2 Remodulation attacks**

Since lossy compression and denoising have been widely presented in the literature, with some applications of low bit rate coding and image enhancement, respectively; it is not incredible that they are also famous attack tools for the watermarking community. On the other hand,

remodulation attacks are a rather fresh theory unique to the watermarking attacks. A systematic remodulation attack was first demonstrated in [32]. In this algorithm, the watermark was forecasted using subtracting from the host stego image to the median filtered version of stego image. The forecasted watermark was also truncated, high-pass filtered, and the subtraction is done from the stego image with a constant amplification parameter with2. Since the median filtering mainly takes away the noise in the high-frequency section, the low-frequency section cannot correctly estimate the value according to this filter. In the situation of a highly consonant between the amplification parameter and the estimated watermark, the attacks have the guidance to a diminishment in extensive correlation in the matched filter with decoding.

An almost equivalent attack with weighted mean forecasting was introduced in [26]. In this work, authors reported their success at removing watermarks generated by the watermarking strategy introduced in [78] and the Digimarc commercial software. In addition, in [66], a Wiener attack is presented. The presented attack comprises three steps: forecasting of the watermark according to the Wiener filter, subtracting from the stego with some strength parameter to the estimated watermark, and adding stationary Gaussian noise. In [50], the impact of the attacks is discussed from the information-theoretic point of view and it is concluded that the attack of additive white Gaussian noise can be optimal asymptotically with respect to removing the watermark when the intensity of the noise is big in comparison to the energy of the watermark.

*6.1.3 Averaging and collusion attacks*

In this group, other attacks are collusion attacks and statistical averaging. With respect to the collusion attacks, numerous examples of the same data are attainable, but the attacked data set is constructed by possessing only a little section of each data set and reconstructing a novel attacked data set from these sections at this time. The latter illustrates an attack where many samples of a precondition data set, each time logged in with a different secret key or distinctive watermark, are averaged to evaluate the attacked data. For example, each frame can be inserted using a different key or a different watermark into video watermarking schemes. If the amount of data set is sufficiently huge, the inserted watermark cannot be discovered anymore supposing that it will output zero mean on average. In [20], collusion and the averaging attacks are discussed in using videos and complementary countermeasures are recommended. The other kind of attack that diminishes the decoding and detection of the watermark is the mosaic attack [55]. The attack was produced in the structure of automatic copyright protection frameworks that investigate the Internet and download images for checking the existence of the watermarked images on pirate websites. The mosaic attack does not attempt to remove the watermark with some image processing approaches, but rather it leads to producing problems for the watermark detection splitting the image into the small fragments.

***6.2 Geometrical attacks***

Compared to the removal attacks, geometric deformation attacks do not plan for the removal inserted watermark, but for distortion of it through temporal or spatial transformations of the stego contents. The attacks are normally described as follows: the detected watermark loses synchronization with the inserted information. The most famous integrated software versions for geometrical attacks are Stirmark [56] and Unzign watermark removal software from 1999. The global attacks are scaling, rotation, translation, change of aspect ratio, and shearing a link up with a kind of extensive affine transformation. The translation /cropping and column/line removals are also merged in Stirmark. Unzign presents local pixel jittering and is extremely efficient to attack watermarking schemes in spatial domains. Stirmark presents both local and global geometric distortions. Most current watermarking approaches are robust against these attacks owing to the application of particular synchronization procedures. If the robustness of global affine transformations is a little or a lot a resolved problem, the local random transformations integrated by Stirmark always remain an open issue almost for all methods. The random bending attacks exploit the background that the human visual system is insensitive towards local affine modifications and shifts. Thus, the locally shifted, rotated and scaled pixels are without distortions in significant visual aspects. The thesis will also discuss dedicated

attacks, which intend to test the efficiencies of proposed algorithms.

*6.3 Cryptographic attacks*

Cryptographic attacks are quite equivalent to the attacks applied in cryptography. There are the seriously forced attacks which intend to discover secret information using the exhaustive searches. Ever since numerous watermarking systems utilize a secret key, it is greatly significant to use keys with a safe length. In addition, another attack is the so-called Oracle attacks in this category [13] and [53], which is able be applied to produce a non-watermarked image while a device of a watermark detector is attainable..

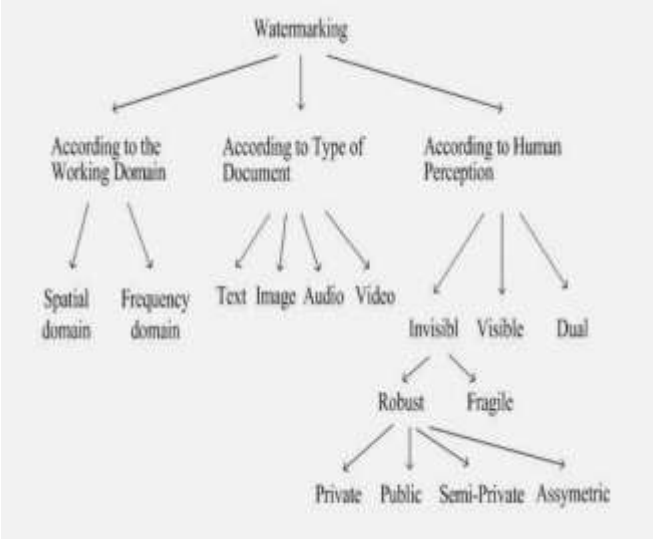
***6.4 Protocol attacks***

The protocol attacks intend to attack the definition of the watermarking applications. The protocol attack was introduced by [19]. They present the structure of unidirectional watermark and demonstrate that watermarks requisite for being non-invertible in applications of copyright protection. The concept of inversion comprises of the truth that attackers who have a copy of the stego contents can represent that the data also includes the attackers' watermark using subtracting to his own watermark information. The activities can produce an ambiguity's condition with respect to the authentic ownership of the contents. The prerequisite of non-inevitability on the watermarking system suggests that it should not be potential to detect or extract a watermark from non-watermarked images.

*6.5 Image Shifting and Line Deletion*

The attackers may change the watermarked image nearby vertically and horizontally, or remove an entire line of pixels, to distort the watermark information delivered. For the embedding watermarks in the VQ or DCT domains, image shifting may result in the algorithm of extracting the watermark to miss the
resynchronization of the watermarked images. How to acquire an acceptable quality in the watermarked image and to preserve the capability for recovering the embedded watermark with the image shifting scheme is another topic for robust watermarking

It is the most important application of digital watermarking. For copyright protection of digital content, copyright information, signature, copyright message, or logo image are inserted or embedded in digital content to be protected. The embedding
algorithm incorporates copyright message which can then be extracted by the extraction algorithm to prove ownership. Although copyright notice does not guarantee the protection of copyright but still it is used. Generally, books, images, audio, and videos contain copyright notices, sometimes visible and sometimes invisible. It is necessary to achieve very high level of robustness
when embedding watermark for copyright protection. Attackers can remove the copyright information through intelligent manipulation of the
contents as image cropping, segmentation of videos, modifications in audio, and rephrasing the text. Hence, it is necessary to embed copyright information in each and every piece of copyright content.



## Digital Watermarking Algorithms

The watermarking algorithms (techniques) can be performed either in
differential operators are comparatively evaluated. Laplacian obtains the highest percentage of correct scale detection. The ratio of the scales, at which the extreme were found for corresponding points in two rescaled images, is equal to the scale factor between the images. The characteristic scale of a local image structure is the scale parameter at which the Laplacian function attains a local maximum over scale factors.
Generally, the Laplacian of Gaussian filter centered on zero with Gaussian standard deviation $\sigma$ has the following form:
compressions. It is shown that SIFT detector has a good potential to be used in watermarking. In this part the comparative evaluation of the scale-invariant feature point detectors: SIFT and Harris-Affine, will be done. The aim of this comparison is to show which feature point detector gives more robust
feature points under different distortions. These points will be used later for image watermarking. The software implementation of these feature point detectors is used. Among them are
non-geometrical operations like:

compressions (JPEG, JPEG2000), filtering operation (Gaussian, median, wiener, and trim mead mean), noise addition (salt' n pepper or Poisson) or geometrical distortion like: rotation, scaling, cropping or combination of them. These images will be referred as distorted images. The feature points will be extracted on the test image and on its distorted version using both feature extraction methods. It will be measured how many corresponding feature points can be found on However, in our experiments we will not observe the total number of extracted feature points. We will reduce it to the set of feature points with the largest characteristic scale.. The synchronization information will be embedded into the circular neighborhood of the feature point, with radius proportional to the characteristic scale. From this point of view it was more reasonable to observe in our experiments only the feature point with the largest characteristic scale.

The whole procedure is performed in the following steps:

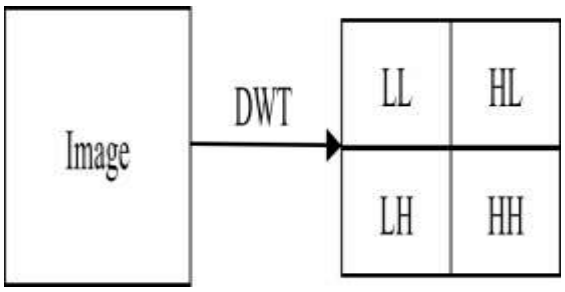
1. The feature points will be extracted on original and on distorted image using SIFT and Harris-Affine feature point detectors;
2. For every feature point extracted with this two detectors its characteristic scale will be computed;
3. The points from the same image will be sorted in descending order by the characteristic scale and first i ($I \in \{10, 20, 30\}$) points from this set will be selected.

### Discrete Wavelet Transform(DWT)

Discrete Wavelet Transform (DWT) gives a multi resolution representation of the image. This representation provides a simple framework for interpreting the image formation. The DWT analyses the signal at multiple resolution. When we apply the DWT to an image, it divides the image into two quadrants, i.e. high frequency quadrant and low frequency quadrant. This process repeats until the signal has been entirely decomposed. If we apply 1-level DWT on two dimensional image, it divides it into four parts, i.e

- *LL:* It consists the low frequency details of the original image. We can say that approximation of the image lies in this part.
- *LH:* It consists vertical details of the original image. *HL:* It consists the horizontal details of the original image.
- *HH:* It consists high frequency details of the original image.

Since we know that the detail of original image lies in low frequency coefficients, so we embed the watermark into low frequency coefficients If we apply IDWT, we can reconstruct the original image from the decomposed




**Properties of the wavelet transform:**

The wavelet transform decomposes an image into three spatial directions i.e. the horizontal HL, the vertical LH and the diagonal HH. At each level of decomposition the magnitude of the DWT coefficients is larger in the lowest Sub bands ("approximation" LL sub-band), and smaller for other sub bands ("detail" Sub bands: HL, LH and HH). The most significant coefficients in a sub band are those with large magnitudes. For an arbitrary image the high resolution sub bands help in locating the edge and texture patterns.

Watermarking in DWT domain has a number of advantages over other transforms, namely, the Discrete Cosine Transform (**DCT**)

1. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different level of resolution and can be sequentially processed from low resolution to high resolution.
2. The DWT is closer to the human visual system than the DCT, since it splits the signal into individual bands, which can be processed independently.
3. The distortions introduced by wavelet domain coding with high compression ratio are less annoying than those introduced at the same bit rate by the DCT. In the JPEG case, block-shaped distortions are clearly visible, since image coding based on the DCT usually operates on independent 8x8 blocks.

Watermarking schemes put more watermark energy into the large DWT coefficients, thus affecting mostly regions, like lines and texture on which the human visual system is not sensitive too.

4. DWT has spatial frequency locality, which means if the watermark is embedded into the DWT coefficients it will affect the image locally. Hence a wavelet transforms both frequency and spatial description for an image.
5. DWT has spatial frequency locality, which means if the watermark is embedded into the DWT coefficients it will affect the image locally. Hence a wavelet transforms both frequency and spatial description for an image.
6. .

## Spatial Domain Techniques

Many spatial techniques are based on adding/ subtracting fixed amplitude pseudo noise (PN) sequences to an image. PN sequences are also used as the "spreading key" when considering the host media as the noise in a spread spectrum system, where the watermark is the transmitted message. These approaches modify the least significant bits (LSB) of the host data on the assumption that the LSB data are visually insignificant. The watermark is generally recovered using knowledge of the PN sequence (and perhaps other secret keys, like watermark location) and the statistical properties of the embedding process. Two LSB techniques are described in Schyndele

### Discrete Fourier Transform

Discrete Fourier Transform (DFT) offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding.

In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is embedded. The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermar image. After this, detector is used to extract the embedded spread spectrum watermark

## Watermarking Attacks

When the watermarked media is transmitted, several attacks take place on that watermarked media. These attacks may be given as:

- *Removal Attack:* In this, the unauthorized user tries to remove the watermark i.e. secret information from the watermarked data.
- *Interference Attack:* In these types of attacks, the noise is inserted to the watermarked media. Some examples of this category are averaging, quantization, compression etc.
- *Geometric Attack:* These types of attacks can change the geometry of the image. The examples of this category are cropping, rotation etc.
- *Low Pass Filtering Attack:* This type of attack takes place when we pass the watermarked data from a low pass filter.

## Discrete Cosine Transform Techniques

In the very early days, Discrete Cosine Transformation was widely studied by the source coding community in the context of JPEG and MPEG compression Wallace (1992); Pennebaker and Mitchell (1992); and Rao and Yip (1990). Later, it was also considered to embed a message inside images (Koch and Zhao, 1995; Zhao, 1996) and videos (Matsui and Tanaka, 1994). The main arguments for using DCT in watermarking are the following:

Embedding rules operating in the DCT domain is often more robust to JPEG and MPEG compression; thus the watermark designer can prevent JPEG/MPEG attacks more easily.

The studies on visibility (i.e., visual distortions) can be reused; these studies help to predict the visible impact of the watermark on the cover-image.

Watermarking in the DCT domain offers the possibility of directly realizing the embedding operator in the compressed domain (i.e., inside a JPEG or MPEG encoder) in order to minimize the computation time

## Fractal Transform Techniques

Though a lot of work has been done in the area of invisible watermarks using the DCT and the wavelet -based methods, a relatively few references exist for invisible watermarks based on the fractal transform. The reason for this might be the computational expense of the fractal transform. Discussions of fractal watermarking methods were presented in Puate and Jordan (1996 November), Roche and Dugelay (1998) and Bas et. al., (1998 October). Puate and Jordan (1996 November) used fractal compression analysis to embed a signature in an image. In fractal analysis, similar pattern were identified in an image and only a limited amount of binary code can be embedded using this method. Since fractal analysis is computationally expensive and some images do not have many large self-similar patterns, the technique may not be suitable for general use**.**

## Feature Domain Techniques

These techniques focused on image region, boundary and characteristics, like flat regions, textures, and edges etc., for watermarking. This gives an additional advantage in terms of detection and recovery from geometric attacks compared to other methods. Also, these algorithms may be designed so that selective robustness to different classes of attacks is obtained. As a result, watermark flexibility will be improved considerably.

Kutter et. al., (1999 October) used feature point extraction and the Voronoi diagram as an example to define region of interest (ROI) to be watermarked. The feature extraction process is based on a decomposition of the image using Mexican-Hat

wavelet. The stability of the method proposed in Kutter's work depends on the features points. These extracted features have the drawback that their location may change by some pixels because of attack or during the watermarking process which will cause problems during the detecting process. Kutter classified this technique as second generation watermarking.

**Background**

digital watermarking are applied in security-critical applications, one needs to account for the presence of an attacker. This adversary may try to attack the learning/watermarking process and thereby impact the confidentiality, integrity, and availability of the application. This section provides a basic introduction to the motivation and threat scenarios in machine learning and digital watermarking, before Section 3 systematizes them under a common notation. A reader familiar with one of the two fields may directly proceed to Section

## Conclusion

The objective of this work was to present a novel watermarking technique for colored images with high robustness without compromising the quality of the watermarked image. The state-of-the-art technique developed is cogent to incorporate both colored watermarks and text watermarks and resulted in high imperceptibility, excellent quality of watermarked image, greater sustenance to image compression like JPEG compression. The sustenance of the technique to common image manipulations like cropping, median filtering, Gaussian filtering, color replacement etc., that are done from various sophisticated image manipulating tools, is promising.

To meet the objective, a thorough literature survey has been done. It has been concluded that the digital watermarking can be achieved by using either transform techniques or by directly embedding the watermark into the spatial domain and each system has their corresponding advantages and limitations. The watermarking scheme that modifies the LSB of the data using a fixed magnitude sequence are (a) quite simple and least complicated thus computationally efficient; (b) highly sensitive to signal processing operations and are easily corrupted; and (c) can be decoded very easily. The watermarking scheme that uses fractal transformation are (a) computationally expensive; (b) only limited amount of binary code can be embedded; and (c) practically not suitable for general use. The watermarking algorithms that uses transform domain are (a) computationally better than fractal ones; but (b) cannot survive most image processing operations and geometric manipulations whereas feature domain watermarking algorithms suffer from problems of stability of feature points when exposed to an attack.

Hence, based on the literature study and the challenges, a model for colored image watermarking had been designed that can encode multiple copies of holographic logo inside the host image without significantly compromising the image quality. The redundant copies of the watermark provide robustness against cropping etc. as traces can be extracted successfully. The use of holographic logo is inspired by the fact that it conveys more information than an uncorrelated sequence of binary numbers as is done prominently to reduce the level of noise and maintain image quality.

The algorithm, based on *model for colored image watermarking*, embedded multiple copies of watermark uniformly throughout the host image thus achieving high number of insertions. The insertions were image independent and only depends on the size of the host image i.e. bigger the host image more number of watermarks can be incorporated. The extracted watermark from an unhampered image was of high quality but sustenance to JPEG compression was very poor. The quality of the image also deteriorated as flat and featureless regions showed a significant amount of distortion. The algorithm was also tested with text watermark. The results revealed same drawbacks and highlighted the need for further improvement

In this paper it have represented various aspects related to digital watermarking. The paper defines the meaning of digital watermarking, its applications and various watermarking techniques which help the new researchers in the field of digital watermarking. It also give the comparisons of various watermarking techniques with their advantages and disadvantages and also defined the performance measurement of images.

As we can see that digital watermarking is very useful method for digital data authentication. It ensures the protection of copyright and authentication. This paper gives an overall analysis of various types of digital watermarking methods. In this paper we have discussed different methods such as spatial domain methods and transform domain method which consists DCT, DWT and DFT. We have discussed the pros and cons of these methods. From a research point of view, this technology is an interesting field because many techniques are emerging for protection of data and many still have to come

# References


- Anderson, R. J., and Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal of Selected Areas in Communications (Special issue on copyright & privacy protection.), vol. 16(4) pp. 474–481
- Baker, G.L. and Gollub, J.P. (1996). Chaotic dynamics: an introduction. *Cambridge University Press.* 2e.
- Barni, M., Bartolini, F., Cappellini, V., and Piva, A. (1997). Robust watermarking of still images for copyright protection. *13th International Conference on Digital Signal Processing Proceedings,* DSP 97, vol. 1, pp. 499-502.
- Barni, M., Bartolini, F., Cappellini, V., and Piva, A. (1998). A D.C.T.-domain system for robust image watermarking. *Signal Processing*. European Association for Signal Processing (EURASIP), vol. 66(3) pp. 357–372.
- Bas, P., Chassery, J., and Davoine, F. (1998, October). Using the fractal code to watermark images. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 1, pp. 469-473.
- Bassia, P., and Pitas, I. (1998). Robust audio watermarking in the time domain. *9th European Signal Processing Conference (EUSIPCO'98),* pp. 25–28.
- Bassia, P., Pitas, I., and Nikolaidis, N. (2001). Robust audio watermarking in the time domain. *IEEE Transactions on Multimedia*. vol 3(2) pp. 232-241.
- Baudry, S., Nguyen, P., and Maitre, H. (2000, October). Channel coding in video watermarking: Use of soft decoding to improve the watermark retrieval. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 25-28.
- Belkacem, S., Dibi, Z., and Bouridane, A. (2007). Color image watermarking based on chaotic map. *Proceeding of 14th IEEE International Conference on Electronics, Circuits and Systems, Marrakech,* ICECS 2007, pp. 343-346.
- Belkhouche, F., and Qidwai, U. (2003). Binary image encoding using 1D chaotic map. *IEEE Region 5 Annual Technical Conference,* pp. 39-43.
- Bender, W., Gruhl, D., Morimoto, N., and Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal,* vol. 35(3 & 4), pp. 1-24.
- Berghel, H., and Gorman, L. (1996). Protecting Ownership Rights through Digital Watermarking. *IEEE magazine Computer,* vol. 29(7), pp 101–103.
- Boland, F., Ruanaidh, J.O., and Dautzenberg, C. (1995). Watermarking digital images for copyright protection. *Proceeding of IEE International Conference on Image Processing and Its Applications,* pp. 321-326.
- Boney, L., Tewfik, A. H., and Hamdy, K. N. (1996). Digital watermarks for audio signals. *IEEE- International Conference on Multimedia Computing and Systems, Hiroshima, Japan.*, pp. 473–480.
- Bors, A., and Pitas, I. (1996, September). Image watermarking using DCT domain constraints. *International Conference on Image Processing Proceedings,* ICIP 96, pp. 231-234.

- Bors, A., and Pitas, I. (1998). Image watermarking using block site selection and D.C.T. domain constraints. *Optics Express*. vol. 3(12) pp. 512–523.
- Brassil, J.T., Low, S., and Maxemchuk, N.F. (1999, July). Copyright protection for the electronic distribution of text documents. *Proceedings of IEEE,* vol. 87(7), pp.1181- 1196.
- Bruyndonckx, O., Quisquater, J.J., and Macq, B. (1995). Spatial -method for copyright labeling of digital images. *Proceeding of IEEE Nonlinear Signal Processing Workshop,* pp. 456-459.
- Canny, J. (1986). A computational approach to edge detection. *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 8(6), pp. 679-698.
- Chae, J. J., and Manjunath, B.S. (1998, January). A robust embedded data from wavelet coefficients. *Proceeding of SPIE, Electronic Imaging, Storage and Retrieval for Image and Video Database,* vol. 3312, pp. 308-317.
- Chae, J.J., and Manjunath, B.S. (1999). Data hiding in video. IEEE, pp. 311-315.
- Chae, J.J., Mukherjee, D., and Manjunath, B.S. (1998). A robust data hiding technique using multidimensional lattices. *Proceedings IEEE International Forum on Research and Technology Advances in Digital Libraries*, ADL 98, pp.319-326.
- Chang, L.W., and Moskowitz, I. S. (1997). Critical Analysis of Security in Voice Hiding Techniques. *Information and Communications Security – First International Conference, Beijing, China, ICICS'97*, pp. 203-216.
- Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1995). Secure spread spectrum watermarking for multimedia. *Technical Report 95-10, NEC Research Institute,* pp. 1-33.
- Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1996, September). Secure spread spectrum watermarking for images, audio and *video. International Conference on Image Processing Proceedings,* ICIP 96, vol. 3, pp. 243-246.
- Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1997, December). Secure spread spectrum watermarking for multimedia. *IEEE Transaction Image Processing,* vol. 6(12), pp. 1673-1687.
- Cox, I.J., Kilian, J., Leighton, T., and Shamoon, T. (1996). A secure, robust watermark for multimedia. *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 183–206, 1996.
- Craver, S., Memon, N., Yeo, B., and Yeung, M. (1997, October). On the invertibility of invisible watermarking techniques. *International Conference on Image Processing Proceedings,* ICIP 97, pp. 540-543.