Digital Watermarking: A Tutorial

Dr. Vipula Singh
Professor and Head of Electrical and Computer Engineering Department
Geethanjali College of Engineering and Technology, Hyderabad India

Abstract—**Due to high speed computer networks, the use of digitally formatted data has increased many folds. The digital data can be duplicated and edited with great ease which has led to a need for effective copyright protection tools. The process of embedding additional data along with the digital audio, images and video is called digital watermarking. A number of watermarking techniques have been proposed in literature. This paper is a tutorial in general watermarking principles and focuses on describing various watermarking techniques.**

***Index Terms*—Digital watermarking, Copyright protection, digital right management**

I. INTRODUCTION

In recent times, due to great developments in computer and internet technology, multimedia data i.e. audio, images and video have found wide applications. Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing multimedia data. Encryption of multimedia products prevents an intruder from accessing the contents without a proper decryption key. But once the data is decrypted, it can be duplicated and distributed illegally. To enforce IP rights and to prevent illegal duplication, interpolation and distribution of multimedia data, Digital watermarking is an effective solution. Copyright protection, data authentication, covert communication and content identification can be achieved by Digital watermarking.

Digital watermarking is a technique to embed copyright or other information into the underlying data. The embedded data should maintain the quality of the host signal. In order to achieve the copyright protection, the algorithm should meet few basic requirements

i) Imperceptibility: The watermark should not affect the quality of the original signal, thus it should be invisible/ inaudible to human eyes/ ears.
ii) Robustness: The watermarked data should not be removed or eliminated by unauthorized distributors, thus it should be robust to resist common signal processing manipulations such as filtering, compression, filtering with compression.
iii) Capacity: the number of bits that can be embedded in one second of the host signal.
iv) Security: The watermark should only be detected by authorized person.
v) Watermark detection should be done without referencing the original signals.
vi) The watermark should be undetectable without prior knowledge of the embedded watermark sequence.
vii) The watermark is directly embedded in the signals, not in a header of the signal.

All these requirements are often contradictory with each other and we need to make a trade-off among them. For example increasing data rate in watermarking system results in quality degradation of the watermarked signal and decreases the robustness against attacks. Imperceptibility and robustness are the most important properties for many applications. These conflicting requirements pose many challenges to design of robust watermarking.

The approach of digital watermarking has been employed to protect intellectual property of audio, images and video data [8, 10, 11, 12]. An invisible watermarking technique in spatial domain is suggested in [1, 2, 3] and in wavelet domain is suggested in [8]. Visible watermarking technique in frequency domain is suggested in [4] whereas dual domain technique is suggested in [5] for images and for audio in [3]. Invisible watermarks can be broadly divided into two types, robust and fragile, most of the research and applications focus on robust watermarks [3, 26]. They are generally used for copyright protection and ownership verification because they are robust to nearly all kinds of image processing operations.

This paper is organized as follows: Section 2 describes general framework, requirements, types and applications of watermarking. Section 3 covers various algorithms of Image watermark and section 4, 5 and 6 deal with audio, video and text watermarking respectively. Finally section 6 concludes the paper.

II. GENERAL FRAMEWORK OF WATERMARKING

Watermarking is the process that embeds data called a watermark into an image or audio or video. The general watermarking framework is in figure 1. The watermark can be detected and extracted later from the carrier (cover). It can contain information such as copyright, license, authorship etc. A simple example of a digital watermark is a "seal" on the image to identify the ownership. Any watermarking algorithm consists of three parts:

a) The **watermark**, which is unique to the owner.
b) The **encoder** for embedding the watermark into the data.
c) The **decoder** for extraction and verification.

2.1 Types of watermarking:

According to the **type of documents** to be watermarked, the watermarking techniques can be divided into four types:

a) Image Watermarking,
b) Video Watermarking,
c) Audio Watermarking,
d) Text Watermarking,

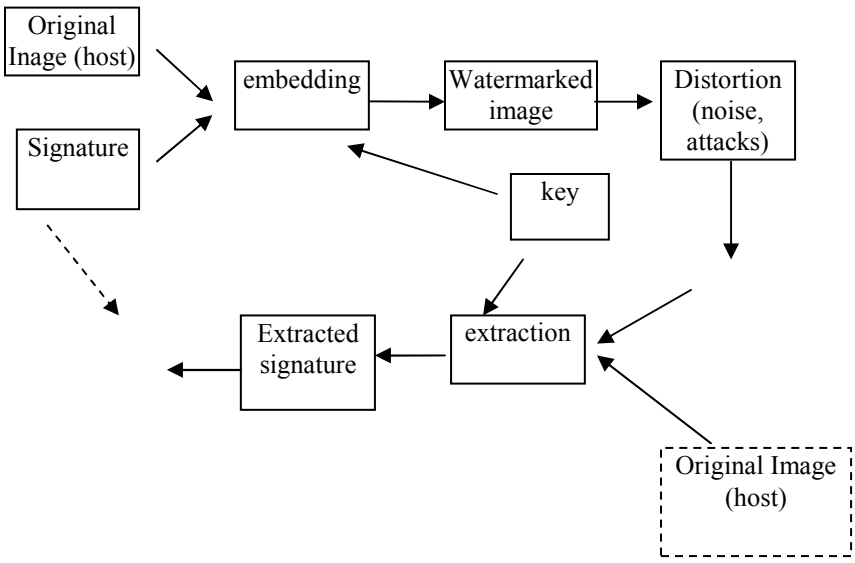


Fig 1. Digital watermarking, a general overview

According to **Human Perception**, the watermarking techniques can be divided into three types
a) Visible Watermark,
b) Invisible Watermark
c) Dual Watermark

Visible watermark is a translucent overlaid into an image and is visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection. Whereas an invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images. Dual watermark is the combination of visible and invisible watermark. An invisible watermark is used as a backup for the visible watermark.

According to **Working Domain**, the watermarking techniques can be divided into two types
a) Spatial Domain Watermarking Techniques
b) Frequency Domain Watermarking Techniques

In spatial domain techniques, the watermark embedding is done on image pixels while in frequency domain watermarking techniques the embedding is done after taking image transforms. Generally frequency domain methods are more robust than spatial domain techniques.
According to the watermarking **extraction process**, techniques can be divided into three types
a) Non-blind
b) Semi-blind
c) Blind
Non-blind watermarking schemes require original image and secret key for watermark detection whereas semi-blind schemes require secret key and watermark bit sequence for extraction. Blind schemes need only secret keys for extraction.

2.2 Attacks on watermarks:

A watermarked image is likely to be subjected to certain intentional and unintentional manipulations such as compression, noise, cropping, filtering etc. Following are some of the manipulations

a) The compression schemes like JPEG and MPEG degrades the data quality, thus possibly altering the watermark.
b) Geometric operations like rotation, translation, scaling and cropping distort data and possibly alter the watermark.
c) Signal Processing Operations like D/A, A/D conversion, re-sampling, re-quantization, dithering, linear filtering, non linear filtering etc.
d) Printing and rescanning, re-watermarking, forgery are some of the intentional attacks which alter the watermark.

2.3 Digital watermarking applications:

a) Copyright protection: Visible watermarking is used for copyright protection which is the most important watermarking application [37, 39]. The owner can protect the data audio, image or video from being used commercially if it is available on internet. The ownership mark should be clearly visible in such cases. Copyright protection requires high level of robustness so that the embedded watermark can not be removed without data distortion. This watermark is extracted to show as proof if someone claims the ownership of the data.

b) Finger Printing: Finger printing is similar to giving serial number to any product. Each distributed multimedia copy is embedded with a different watermark. The objective is to convey the information about the legal recipients. A robust watermarking algorithm is required for this application. Watermark is embedded in digital data to trace the source of illegal copies. Information related to customer like serial number or customer identity information is used as watermark. If any illegal copy is found the source of illegal copy can be found by extracting the watermark.

c) Content Authentication (integrity protection): Invisible watermark is an evidence of ownership. The objective of this application is to detect modification in data. To verify the authenticity of the received data watermark is embedded in host data. A fragile watermarking algorithm is required in this

case. This watermark helps in finding the tampered regions and estimating by how much and how the data is altered. [28, 40]

d) Broadcast Monitoring: Watermark is embedded in commercial advertisements. Automated monitoring system can verify whether the advertisements are broadcasted as contracted or not. The main use of broadcast monitoring is to protecting the valuable TV products like news items from illegal transmission.

e) Indexing: Comments and markers or key information related to the data is inserted as watermark. This watermark information is used by a search engine for retrieving the required data quickly and without any ambiguity.

f) Medical Applications: Patient's information is inserted as watermark in medical images. It helps in avoiding ambiguities in searching the medical records.

III. IMAGE WATERMARKING

In the field of digital Watermarking, lot of research work has been carried out [1-10]. As discussed earlier, image watermarking has been done in many ways in literature. Most important of them are spatial domain and frequency domain techniques.

3.1 Spatial Domain Watermarking Techniques

In 1994, Bender et al [11] described two watermarking schemes. First method is called Patchwork where n pairs of image points (a_i, b_i) are randomly chosen. The brightness is increased by one unit at a_i while decreasing the brightness of b_i. The second watermarking method is called texture block method. In this method, a region of random texture pattern is found in the image is copied to an area of image with similar texture. The texture region is recovered by using autocorrelation function. The major drawback of this technique is that it is suitable for the images that have predominantly texture areas. Thus this technique is not suitable for audio data and for images having only text.

Dinu Coltuc et al [34] proposed a simple integer transform called reversible contrast mapping (RCM) that is applied to pairs of pixels. This is a spatial domain reversible watermarking scheme that achieves high capacity data embedding without any additional data compression stage.

The embedding scheme is based on RCM which is a simple integer transform defined on pairs of pixels. Though LSB of the transformed pixels are lost, RCM is perfectly invisible. A very fast lookup table implementation is proposed by the authors which reduces the computational complexity and makes the scheme appropriate for real time applications. The watermarking technique is robust against cropping.

A technique to embed more information into the input image was proposed by I. Pitas et al. [13]. A binary signature consisting of equal number of zeros and ones act as a watermark. The watermark is embedded in to the image by assigning pixels into one of the two sets. The intensity levels of the pixels in one of the set are altered and the intensity level is not altered in the other set. Watermark detection is done by comparing mean intensity value of the marked pixels against that of not marked pixels. A major advantage of the algorithm is that it does not need the original image for watermark detection.

A dual watermarking technique was suggested by S. P. Mohanty et al. [5]. A visible watermark and an invisible watermark combined is called dual watermark. The invisible watermarking is used for the protection or the backup of the invisible watermark. Following steps as shown in fig 2 (a) are required for the watermarking process:

1) The original image I and the watermarking image W are divided into blocks of same size.
2) For each block, mean μ_n and variance σ_n is computed. μ the mean gray value of the image is also calculated.
3) Watermarked image block is obtained by modifying $i'_n = a_n i_n + b_n w_n$ where
$a_n = \frac{1}{\sigma_n} exp\ (-(\mu_n^{\wedge} - \mu^{\wedge})^2)$
where $\mu_n^{\wedge}$ is normalized value of μ_n
$\mu^{\wedge}$ is normalized value of μ
$\sigma_n^{\wedge}$ is normalized value of σ_n
4) The generated image I' is the visible watermarked image which will be subjected to invisible watermark insertion.
5) Pseudorandom binary sequence is generated and a watermarking image is generated by arranging the binary sequence into blocks.
6) Invisible watermark insertion starts with most significant bit plane (k=0) of the image I'. To generate the k^{th} bit-plane of the watermarked image, watermark is ex–ored with the k^{th} bit-plane of the image I'.
7) Final watermarked image I'' is generated by merging all the watermarked bit planes of the image I'.
8) To make the watermark perceptually invisible, the SNR of the image I'' is calculated. If SNR < threshold, we go back to step 6 with incrementing k by 1 (next lower bit plane). Thus finally dual watermarked image I'' is obtained.

Dorairangaswamy et al [39] proposed an invisible and blind watermarking scheme for copyright protection of digital images. In watermark embedding, each pixel of the watermark image is embedded into the individual blocks of the host image sized 2x2 according to the figure 3. For the extraction process, as the extraction is blind, only watermarked image, size of watermark image and embedding strength is required. Initially watermarked image is divided into 2x2 non overlapping blocks. These blocks are stored as vector and mean of the vector is computed. Mean divided by the embedding strength is used to extract watermark as shown in fig 3.

3.2 Frequency Domain Watermarking Techniques

Watermarking schemes for embedding watermark that resemble quantization noise was suggested by Tanaka et al. [14]. They suggested that as quantization noise is imperceptible to the viewers, watermark is inserted into the image by dithering the image with a dithering matrix. There are several drawbacks of this scheme. The watermark is susceptible to signal processing operation especially re-quantization and geometric attacks like cropping. Further, the

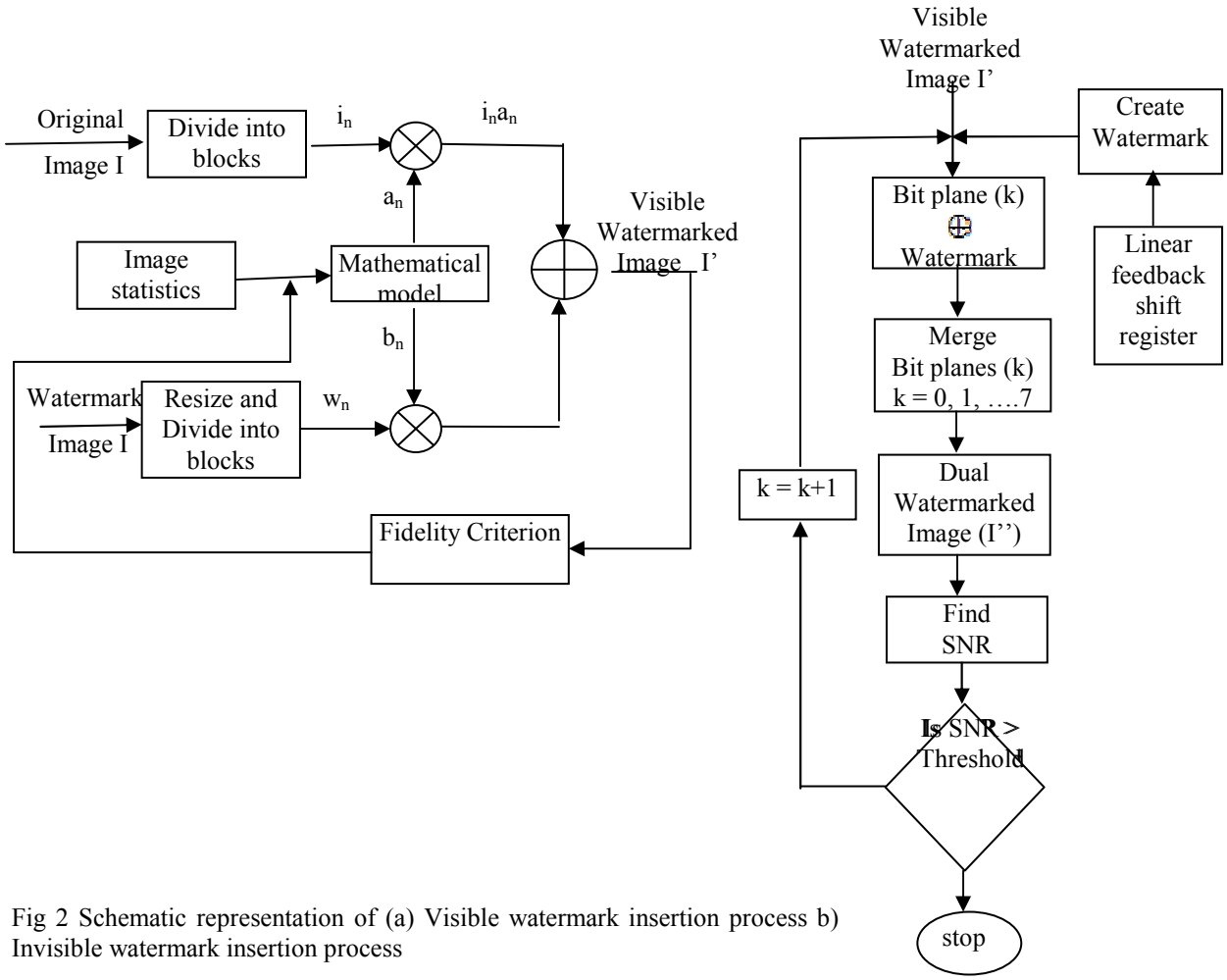


Fig 2 Schematic representation of (a) Visible watermark insertion process b) Invisible watermark insertion process

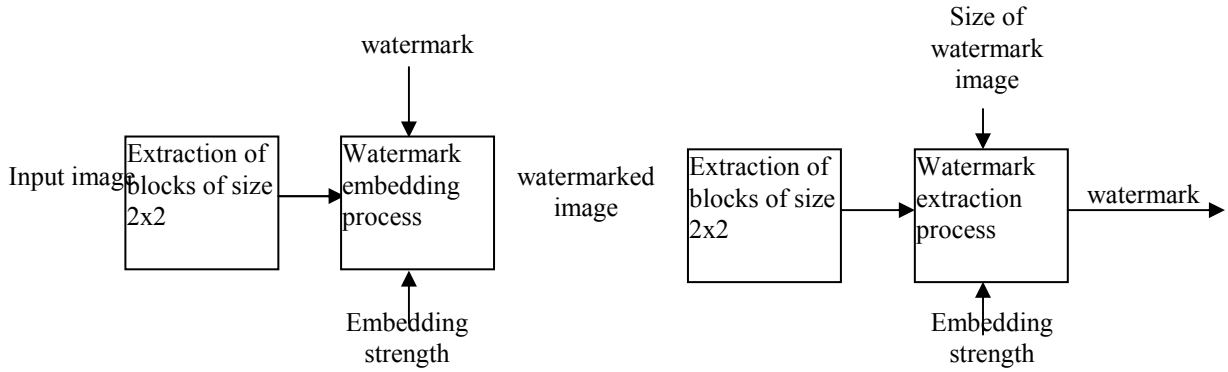


Fig 3 Watermark embedding and extraction process [39]

image is also degraded. Tanaka et al proposed a watermarking method for color images and video. This method applies DCT to 8 x 8 sub-blocks of an image and embeds a watermark in the coefficient quantization module. This scheme may susceptible to re-quantization and dithering and is equivalent to coding the watermark in the least significant bits of the transform coefficients.

An invisible watermark was proposed by I.J.Cox et al. [1, 2, 3]. Spread spectrum like technique was used to insert the watermark into the spectral components of the image.

In spread spectrum communication, one transmits a narrow band signal over a much larger bandwidth such as that signal energy present in any single frequency is imperceptible. Similarly, the watermark is spread over many frequency components so that energy of any component is very small and certainly undetectable. In this method the frequency domain of cover signal is viewed as a communication channel and the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that the transmitted signal must be immune to. The

authors claim that in order for the watermark to be robust, watermark must be placed in perceptually significant regions of the cover signal despite the risk of potential fidelity distortion. Conversely if the watermark is placed in perceptually insignificant regions, it is easily removed, either intentionally or unintentionally by, for example, signals compression techniques that implicitly recognize that perceptually weak components of a signal need not be represented. To make the watermark robust to common signal processing distortions, it should be inserted in the perceptually significant components of the signal. Watermarking insertion process as shown in fig 4 (a) is as follows;

1. DCT of the original image C (treated as cover) is computed.
2. 1000 largest coefficients are chosen which are considered perceptually significant regions of the image.
3. The watermark W=w_1, w_2, w_3…….w_n is a sequence of real numbers generated by the normal distribution with mean zero and variance 1.
4. The watermark is embedded in the spectrum of C using the following equation $c_i' = c_i(1 + \alpha w_i)$. α is the scaling factor (chosen as 0.1)

Watermark extraction algorithm as shown in fig 4 (b) is follows:

1. DCT of the watermarked image C'' is computed.
2. DCT of the original image C is computed.
3. The difference between the two gives the watermark W_i^*
4. Extracted watermark W* is compared with the original watermark using the following equation.

$$\sin(W, W^*) - \frac{W^*.W}{\sqrt{W^*.W^*}} \qquad 1.1$$

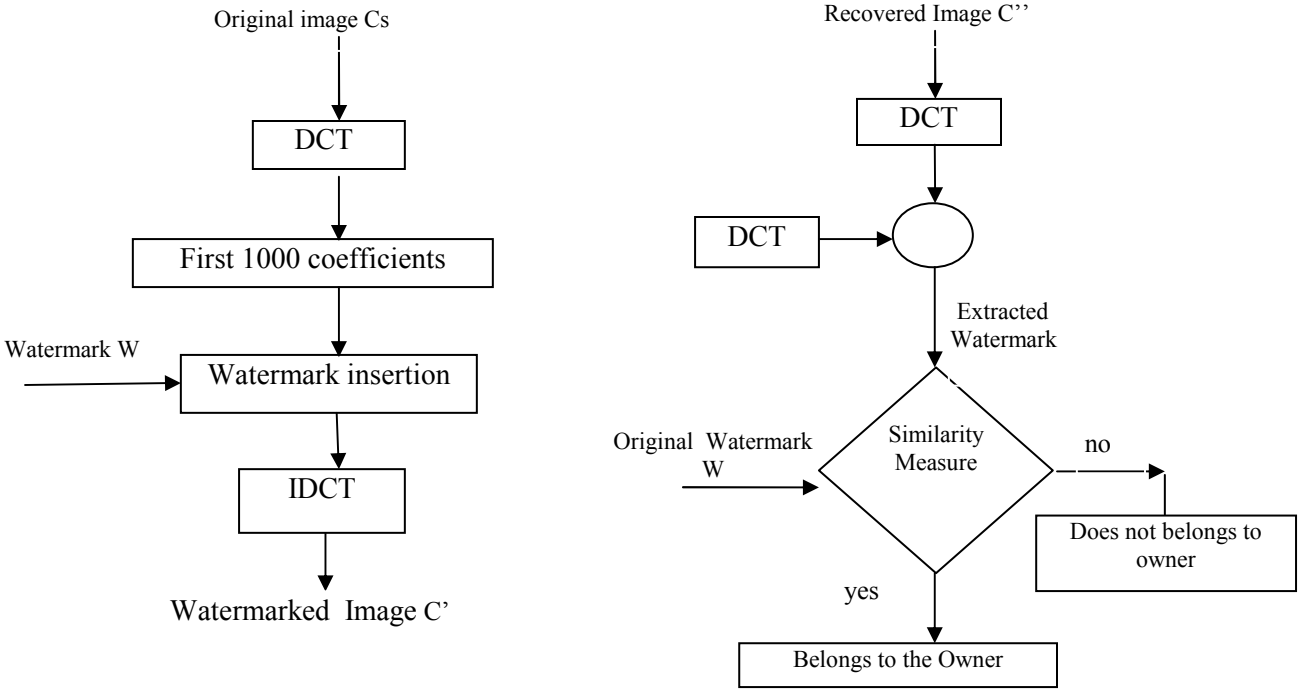
$$Where\ X.Y = \sum_{i=1}^{n} x_i y_j$$

The location of the watermark W in the spectrum of C is known only to the copyright owner. Thus the watermark can be decoded only by the owner which ensures the security of the watermark. N' can be altered by intentional or unintentional attacks to produce N*. With N and N*, a corrupted watermark W* can be extracted and compared with W. A similarity measure is used to compare between W and W'.

The watermark is robust to common signal processing operations and geometric distortion of the images such as A/D and D/A conversion, re-sampling, quantization, compression, rotation, translation and cropping. A major disadvantage of this technique is that it leads to perceptual degradation of the signal. The watermarking scheme can be applied to audio and video signals also.

M.Kankanhalli et al [4] proposed a visible watermark technique by taking the DCT of 8 x 8 blocks of input image as shown in fig 5. Each block was classified into 6 different classes in increasing order of noise sensitivity, such as edge block, uniform with moderate intensity, uniform with high or low intensity, moderate busy, busy and very busy. Different α, β values are assigned to each block. The watermarked image is generated by adding α times input image to β times watermark.

$$z_{ij}' = \alpha z_{ij} + \beta w_{ij} \qquad 1.2$$



a) Watermark insertion process b) Watermark extraction process

Fig 4 Schematic representation of watermarking scheme of [1,2,3]

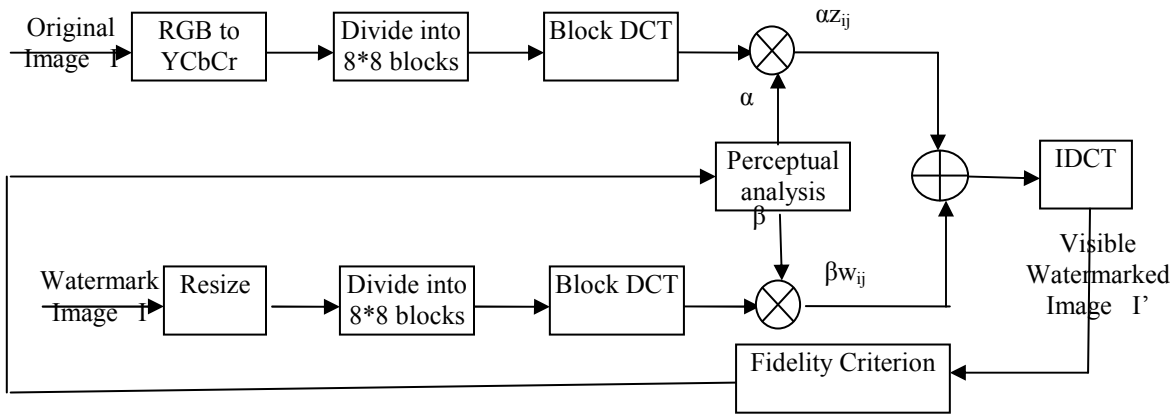


Fig 5 Schematic representation of watermarking scheme of [4]

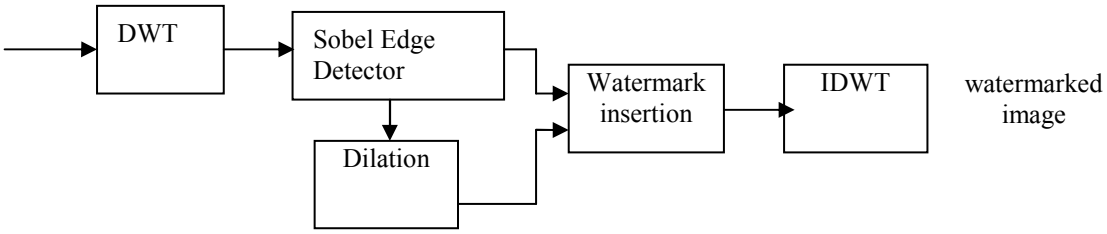


Fig 6 block diagram of watermark insertion process [36]

Where z_{ij} is the DCT coefficients of the original image X and w_{ij} is the DCT coefficient of the watermark. z'_{ij} is the watermarked image.

An invisible spatial domain watermarking technique was proposed by R.B.Wolfgang et al. [19]. A 2-D watermark of size same as the image was added to the input image. Spatial cross correlation is calculated to find the authenticity of the document.

W. Zhu et al. [8] suggested an invisible watermark inserted in the wavelet coefficients. The watermark is added to every high pass wavelet coefficient and thus is visually invisible.

John Ellinas [36] proposed a robust watermarking algorithm using wavelet transform and edge detection whose efficiency depends on preservation of visually significant information. This is carried out by embedding watermark in those sub band coefficients that lie on the edges, where distortions are less noticeable. This technique is robust to common signal processing operations such as compression, filtering, enhancement, rotation, cropping and translation.

Fig 6 shows the overall process of watermark insertion. Initially input image is decomposed to four levels by using Daubechies 8-tap filter. Then from each sub-band perceptually important wavelet coefficients are detected by sobel edge detector. These edges are classified into two groups with respect to a threshold value. Coefficients containing the region around the edges are separated using a morphological dilation operation. The watermark is inserted in detailed sub-bands that contain edge information or to the high frequency coefficients. Thus making the watermark invisible to human eyes.

Watermark detection is performed by correlating the watermarked coefficients of possibly watermarked image with the watermark to be tested for presence as shown in fig 6 Lee et al [33] proposed a high capacity reversible image watermarking scheme based on integer-to-integer wavelet transform. First XxY input image is divided into MxN non overlapping blocks. A set of B_m message bits to be embedded in this block using forward invertible integer to integer wavelet transform. The location map L is a binary matrix that indicates which blocks are watermarked. As a part of side information this is sent to decoder to retrieve the message bits and to reconstruct the original image.

In the decoding process, the decoder has to retrieve the location map first. The watermarked image has to be divided into non overlapping blocks with dimension MxN. Each block is transformed using the same wavelet used in embedding process. Then LSB changeable blocks (found in the location map) are searched in a predefined order.

Based on the location map, the blocks into which the watermark is embedded is sequentially searched. Finally the entire payload is extracted which includes original LSBs and the location map. Thus original image block can be reconstructed back exactly. The authors also show the comparison with other reversible schemes. Fig 7 shows the comparison of the embedding capacity in bpp versus distortion in PSNR of various reversible schemes [33]. As clear from the figure, RS scheme [27] has low embedding capacity as compared to others. In [28, 29, 30, 32] the trade off between capacity and image quality is possible and relatively high data embedding capacity can be achieved. Fig 7.

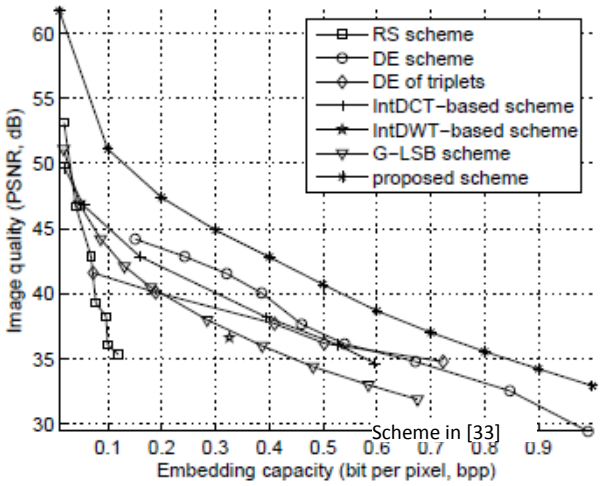


Fig 7 Comparison of embedding capacity in bpp versus distortion in PSNR with existing reversible schemes — RS [27], DE [28], DE of triplets [29], Integer DCT [30], Integer DWT [31], and Generalized-LSB [32] schemes. The test image is the gray-scale Lena [33].

IV. Audio Watermarking

According to the methods of achieving fidelity, audio watermarking can be roughly classified into following categories

1) To embed the watermark in time domain [15,10]

2) To embed the watermark in the perceptually insignificant regions of the signal in spectral domain [20,21] but the weakness of this method is that it is not robust especially against malicious attacks.

3) To embed the watermark as the echo of the original signal [48] which is based on the assumption that Human Audio System (HAS) can not notice it as watermark is treated as noise and HAS can not perceive the added echo.

4) To embed the watermark like spread spectrum technique [1,2,3] which achieves higher robustness.

4.1 Spatial Domain Watermarking Techniques

L. F. Turner [15] proposed a method for watermarking digital audio signals. He suggested substituting bits of identification code to the insignificant bits of randomly selected audio signal. Such a substitution can be done for images also. But the watermark can be easily removed by flipping the least significant bits which contain the identification code.

Bissia et al [10] proposed a time domain method for audio watermarking as shown in fig 8. They proposed to reduce the distortions resulting from watermark embedding by modulating the original signal and then low pass filtering it. The audio signal is divided into segments and each segment is watermarked separately by embedding the same watermark. Watermark signal w $\in$ {1, -1} is generated randomly. A= a_1, a_2, ……a_n is the audio signal to be watermarked. Watermarking is done by modulating the watermark W_i by the audio signal A. $w'_i = \alpha s_i \oplus w_i \;\; i = 0, 1 \ldots\ldots n-1$

Where $\oplus$can be multiplication, power law etc any operation that follows superposition law. $\propto$ is the constant to control the amplitude of watermark signal. Maximum perceived signal distortion limits the maximum allowable watermark amplitude. w_i' is passed through a low pass filter Hamming filter of length L with filter coefficients as b_l.

$$w''_i = \sum_{l=0}^{L-1} b_l w'_{i-1} \qquad 1.3$$

w_i'' is an inaudible watermark signal because the power spectral density (PSD) of w_i'' lies below the PSD of original audio signal.

$o_i = s_i + w_i$'' is the final watermarked signal. For watermark detection, the correlation between the received signal O and the original watermark W is calculated. This watermarking system is immune to time shifting and cropping.

4.2 Frequency Domain Watermarking Techniques

An audio watermarking scheme in Fourier domain is suggested by Arnold [20, 21] in 2001 which uses statistical algorithm. Advantage of this method is that it doesn't need the original audio signal in the detection process.

Audio signal is broken into frames. One bit is embedded by each frame. First step is to take the DFT of the frame. 2N values are assumed to be present in each frame. The embedding process has the following steps:

1. A secret key is mapped and used as a seed of random number generator. Generator starts generating pseudo-randomly two intermixed subsets p={p_i} , i=1,2,….M and subsets q={q_i} , i=1,2,….M of equal sizes where M $\leq$ N.
2. The selected elements $q_i \epsilon Q$ and $p_i \epsilon P$ are altered according to the embedding function below

   $p'_i = p_i + \Delta p_i \quad q'_i = q_i + \Delta q_i$, where Δp_i and Δq_i are pattern generated by secret key. Two patterns are generated for 0 bit and two patterns for 1 bit.

The correct pattern is selected according to the value of bit being embedded. The watermark has to be inaudible, therefore the changes in frequency domain is done carefully.

Hypothesis test is used in watermark detection process. Two test hypotheses are formulated H_0 and H_1. The hypothesis test statistics is a function of two sets P and Q, with the probability density function PDF φ(z) in un-watermarked case and $\varphi_m(z)$

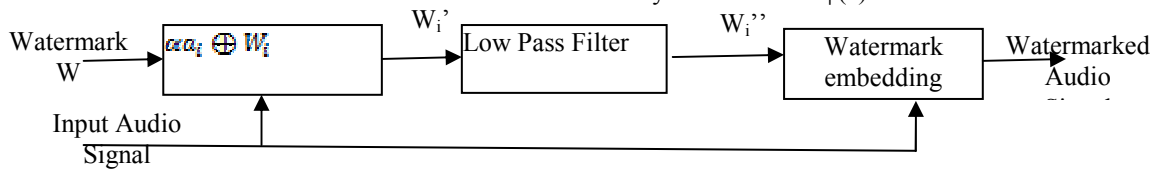


Fig 8 Schematic representation of watermarking scheme of [10]

in watermarked case.

H_0: No embedding of watermark. Z follows PDF $\varphi(z)$

H_1: Embedding of watermark. Z follows PDF $\varphi_m(z)$

Hypothesis testing is used in the detection process. It has to be decided whether the watermark bit is embedded or not. Detection process is as follows:

1. A secret key is mapped and used as a seed to generate random number subsets R and S. if the correct key is used then R = P and S = Q.
2. Probability of correct rejection P_I is decided and the threshold T for type I error is calculated.
3. Sample mean E(z) is calculated using R and S. E(z) is used for hypothesis.

H_0 : E(z) $\leq$ T the watermark bit is embedded.

H1 : E(z) > T the watermark bit is not embedded.

As it is clear from the above procedure, the detection process doesn't require the original audio signal.

Y Tang et al [49] proposed a digital watermark algorithm based on wavelet transform and complex cepstrum transform (CCT) which takes advantage of masking effect of human ears. The embedding scheme as shown in the fig 9 is as follows: 1) Discrete Wavelet Transform is applied to audio signal. 2) Collect all the input coefficients by zig-zag scanning. 3) Cepstral coefficients are calculated using CCT. 4) To improve security watermark is preprocessed by confusion matrix. 5) Watermark is embedded and inverse CCT and inverse DWT is applied to get a watermarked audio. The authors claim that the watermark is robust against common signal processing operations.

4.3 Dual Domain Watermarking Techniques Boney et al [3] suggested the dual domain (time domain as well as frequency domain) watermarking approach based on Human Audio System. The authors suggested shaping the watermark in frequency domain but embedding of the watermark is done in time domain. Two keys k_1 and k_2 are used to generate noise like sequence as watermark. The first key k_1 is author dependent and the second key k_2 is computed from the original audio signal to be watermarked. One way hash function is used on the input audio signal to generate key k_2. These two keys are used to generate watermark which is a noise like sequence. In the detection process, the original audio signal and the key k_2 (generated from the original audio signal) is used to reconstruct the watermark signal.

V. VIDEO WATERMARKING

C T Hsu et al [16] proposed a video watermarked technique based on DCT (Discrete Cosine Transform). For watermark insertion the following are the steps

1) The first frame is divided in 8x8 blocks.
2) DCT is computed for each block.
3) Middle frequency coefficients are chosen.
4) The residual pattern is computed from the chosen middle frequency coefficients.
5) To remove spatial relationship, 2 D pseudo random number traversing method is used to permute image watermark.
6) In order to make watermark invisible, variance of image block and watermark block are sorted and mapped.
7) Foe each of the marked pixel of the permuted watermark, binary residual patterns of the transformed frame is found. Then the DCT coefficients are modified according to the residual mask.
8) The watermarked image is the IDCT value of the result.
9) The relationship between current P frame and its reference frame embeds the watermark.
10) For B frame, the difference between the current B frame and its past and future reference frames gives the residual mask.

The watermarking algorithm is robust to MPEG compression and cropping. Extraction process is the reverse of insertion process. The main disadvantage of the extraction process is that it requires the original frame also.

An object based watermarking technique for video was suggested by swanson et al. [22] in the video, for every object, individual watermark is created. According to the perceptual watermarking characteristics of the video, a pseudorandom sequence is generated which is video dependent and acts as a watermark for each object. The insertion process is as follows;

1. First, for the current frame, spatial (S) and frequency (F) masking values are calculated. To find F, the frequency masking values, DCT of 8*8 blocks in the frame is obtained.
2. Each frame is segmented into blocks (B). This ensures that masking estimates are localized.
3. A part of pseudorandom sequence is then multiplied to frequency masking values of each block.
4. Inverse DCT is computed.

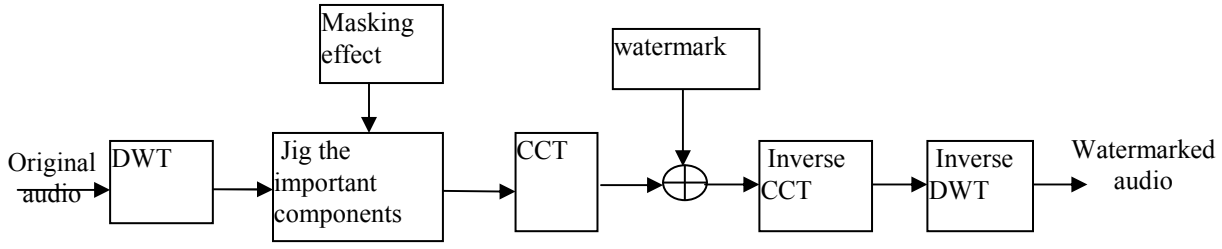


Fig 9 block diagram of watermark embedding [49]

5. Perceptually pseudorandom noise is created by multiplying the result of the above step to the spatial masking values of the frame.
6. This pseudorandom noise is added o the block to get the watermarked block B'.

Detection of the watermark is by likelihood test. Main advantage of the watermarking scheme is that the watermark is statistically untraceable and multiple ownership issue is also resolved. MPEG-4 object based coding frame work can easily incorporate this watermarking algorithm. The algorithm is immune to intentional and unintentional attacks like noise, cropping, MPEG compression, scanning, and printing.

A robust watermarking of mpeg-2 video is presented by B. Girod et al. [23, 24, 25] embedding of the watermark is done in the encoded video or in the MPEG-2 bit stream. The watermark is retreated easily from the codec. A pseudorandom signal which is below the threshold perception is added to the raw video for watermarking. This watermark is invisible and can't be removed without the knowledge of the parameters of watermarking algorithm. The technique of the direct sequence spread spectrum communication is used in watermarking modified signal. The modified signal is produced as per the following equation.

$$s_i' = s_i + a_i b_i n_i \qquad 1.4$$

Where n_i is pseudorandom noise
a_i is amplitude scaling
b_i is embedded bit
a matched filter is used to recover information bit. If the watermark consists of only +1 and -1, it is easier to figure out the watermarked pixel value from several sequences with different watermarks. The watermarking procedure consists of the following steps for each signal block.

1. The watermark data is the spread spectrum information modulated by pseudorandom noise sequence.
2. First DCT of the 8*8 block of the watermark is calculated.
3. 8*8 matrix of DCT coefficients D_n is converted into 1*16 vector by doing zig-zag scanning. D_0 is the DC coefficient value and D_1 to D_{63} are AC coefficients. S_n is the un-watermarked signal and S'_n is the watermarked signal.
4. For the DC coefficients (first coefficient), the watermarked signal is generated by adding the mean value of the watermark block to the mean value of the signal block. $S_n' = S_0 + D_0$
5. For the remaining 63 AC coefficients, the bit stream of the coded signal is searched for the next VLC codeword, the pair (r_m, l_m) belongs to that codeword is identified and thus the position and amplitude of AC DCT coefficients represented by the VLC codeword.
6. $S_m' = S_m + D_m$ is the DCT coefficient of the watermarked signal. This procedure should not increase the bit rate.
7. Let B be the number of bits required to transmit the codeword for (r_m, l_m) (for un-watermarked signal S_m) and B' is the number of bits used to transmit the code word for (r_m, l'_m) (for watermarked signal S'_m). (r_m, l'_m) pair is transmitted if B $\geq$ B' else (r_m, l_m) is transmitted.
8. Repeat steps 3-7 till end of block (EOB) is encountered.

The watermarking scheme in the bit stream domain is less robust as compared to the schemes in pixel domain. The main reason for this is that due to bit rate constraint, only few DCT coefficients of the watermark can be incorporated in 8*8 block. The main advantage of this scheme is less complexity of the decoding process. The watermark is robust against linear and nonlinear attacks like re-quantization, transmission coding, filtering, rotation, scaling etc.

VI. TEXT WATERMARKING

Over past few years, a lot of text data is exchanged in digital form over internet. Very robust copyright protection mechanism is required in these exchanges. Ideal watermarking scheme should be implemented easily, it should be robust and imperceptible. The watermarking scheme must be adaptable to different text formats and information carrying capacity should be high. It should be applicable to print/digital proofs. Brassil et al [12] proposed watermarking techniques for images containing text.

Yong et al [35] proposed a text watermarking algorithm that exploits the concept of word classification and inter word space statistics. The authors extracted features to classify words. Segments were found using several adjacent words and segments were classified using word class information. Some amount of information is inserted into each of the segment classes. The data is hidden by modifying some statistics of inter-word spaces of the segments of same classes.

Text image watermarking and natural languages watermarking are the two ways in which text watermarking is done. Text image watermarking exploits the redundancy in images and limitations of Human Visual System (HVS). The algorithm relies on line-shifting and word shifting. Huang et al [43] developed a word shift algorithm that modifies the inter word spaces that represent a sine wave. The signals are encoded in the phase, amplitude and frequency of sine waves. For signal insertion, spaces between the characters should be adjusted. This algorithm is not robust against attacks such as scanning the document and performing optical character recognition or reformatting the file.

Suganya et al [41] proposed to modify perceptually significant portions of an image to make the algorithm more robust

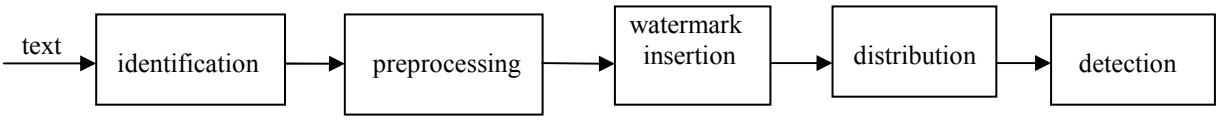


Fig 10 Text watermark insertion and detection scheme [41]

against attacks. Fig 10 shows the insertion method. First text is identified as printed copy or a digital copy, the preprocessing is done. The watermark is hidden in the point's location of the letter i and j. first few bits are used to indicate the length of the hidden bits to be stored. Then the cover medium text is scanned to store a one, the point is slightly shifted up else it remains unchanged.

Natural language watermarking is an emerging technology in the text image security and natural language processing. Additional information in the text is embedded with a goal of subliminal communication and hidden information transport of content and authorship authentication and finally enriching the text with metadata [44]. In studies on natural language watermarking has just started. M Atallah [45] proposed a semantically based technique for information hiding in natural language text. The authors described the technique for embedding a resilient watermark in text by combining security techniques and resources of natural language processing information hiding capacity of English text is improved a lot by modifying the granularity of meaning of individual sentences. But this is suitable for only English language.

A technique for embedding secret data without changing the meaning of the text is proposed in [47] by replacing words in the text by synonyms. This method deteriorates the quality of the document and a large synonym dictionary is needed. Topkara et al [46] proposed syntax based natural language watermarking using the syntactic sentence-paraphrasing. This syntax based technique focuses on the syntactic sentence–paraphrasing. The authors insisted that this approach is useful for natural language watermarking without semantic distortion. M.Y. Kim [42] proposed a method useful for agglutinative languages such as Korean, Turkish etc of which syntactic constituent order is relatively free. The embedding process is as follows: 1) Syntactic parsing is performed and syntactic dependency tree is obtained. 2) Target syntactic constituents are chosen for movement in a sentence and the moving direction is determined. 3) Watermark bits are embedded. It is identified if the movement bit corresponds to watermark bit or not. 4) Then target constituents are moved to determine direction. Then finally a marked sentence is generated from modified syntactic tree. The authors claim that watermarking technique show reasonable performance without semantic and stylistic distortion.

VII. Conclusions

To embed a hidden robust watermark to digital multimedia is the ultimate goal of watermarking system. Generally watermarking schemes have to satisfy two conflicting requirements

a) It must not introduce any distortion in the host signal. That is watermark must be perceptually undetectable.
b) The watermark must be immune against intentional or unintentional attacks or removals.

A variety of techniques in different domains have been suggested by different authors to achieve above mentioned conflicting requirements. All the watermarking techniques are different from each other and are used for differing applications.

In the detection process of some watermarking techniques, the original signal is required. These systems are not suitable for the applications where the original signal is not accessible at the detection or it is unacceptable to disclose it.

To maintain the security of the watermark, it should be embedded into randomly selected regions in some domain of the watermark signal. By doing this, it is difficult to remove the watermark. Randomly selection of the region is done by selecting a sequence of indexes by a key called watermarking key. This key is required in both embedding and detection process. In some algorithms, randomly generated bits are used as watermark.

Copyright owner provides the watermarking key or a combination of information provided. This information is used to generate key from the original signal. In this case, original signal is needed for detection.

In some applications, it is not possible to disclose watermarking key. Then two different keys are used, one for embedding the watermark and other for detection.

In case of audio and video watermarking, the signal has to be divided into frames during embedding process. Then watermarking is done for each frame separately. In some watermarking algorithms, to enhance the robustness of the watermark, same v is embedded into a number of frames. But in some algorithms, different watermarks are embedded in each frame.

Invisible watermarks should be shaped according to the HAS/HVS. Masking characteristics of the input signal should be used.

References

1) I.J.Cox et. al., "Secure Spread Spectrum Watermarking of Images, Audio and Video", Proc IEEE International Conf on Image Processing, ICIP-96, Vol.3, pp 243-246, http://www.neci.nj.nec.com/tr/neci tr 95 10.ps
2) I.J.Cox, et. al., "A Secure Robust Watermarking for Multimedia", Proc. of First International Workshop on Information Hiding, Lecture Notes in Comp. Sc., Vol.1174, pp.185-206, Speinger-Verlag, 1996.
3) I.J.Cox, et al., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, Dec 1997, pp.1673-1687.
4) M. Kankanahalli, et. al., "Adaptive Visible Watermarking of Images", Proc. of IEEE Int. Conf. on Multimedia Computing Systems, ICMCS-99, Cento Affari, Florence, Italy, June 1999.
5) S.P.Mohanty, et al., "A Dual Watermarking Technique for Images", Proc. 7th ACM International Multimedia Conference, ACM-MM'99, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.
6) N. Nikolaids and I. Pitas, "Copyright Protection of on Image Pro- Images Using Robust Digital Signatures",

Proc. IEEE International Conf. on Acoustics, Speech and Signal Processing, ICASSP-96, Vol. 4, pp.2168-2171.
7) N. Nikolaidis and I. Pitas, "Robust Image Watermarking in Spatial Domain", Signal Processing, Vol.66, No.3, pp 385-403.
8) W. Zhu, et al., "Multi-resolution Watermarking for Images and Video", IEEE Tran. on Circuits & Systems for Video Technology, Vol.9, No.4, June 1999, pp.545-550.
9) W. Zhu, et al., "Multi-resolution Watermarking for Images and Video : A Unified Approach", Proc. IEEE International Conf. on Image Processing, ICIP-98, Vol.1, pp. 465-468.
10) Bassia P., Pitas I., and Nikolaidis 2001, "Robust Audio Watermarking in Time Domain", IEEE Trans. On Multimedia, Vol. 3, pp. 232-241.
11) Bender W., Gruhl D., Morimoto N. and Lu A. 1996, "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, No. 3&4, pp. 313- 335.
12) J. T. Brassil, et al., "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications, Vol.13, No.8, Oct 1995, pp.1495-1504.
13) G. Voyatzis and I. Pitas, "Chaotic Watermarks for Embedding in the Spatial Digital Image Domain", Proc. IEEE International Conf. on Image Processing, ICIP-98, Vol.2, pp.432-436.
14) K. Tanaka, Y. Nakamura, and K. Masui, "Embedding secret information into a dithered multilevel image," In Proceedings of the 1990 IEEE Military Communications Conference, pp. 216-220, September 1990.
15) L. F. Turner, "Digital Data Security System" Patent IPN WO 89/08915, 1989.
16) C. T. Hsu and J. L. Wu, "DCT-Based Watermarking for Video", IEEE Trans. on Consumer Electronics Vol.44, No.1, Feb 1998, pp. 206-216.
17) F. Hartung and B. Girod, "Watermarking of uncompressed and compressed Video", Signal Processing, Vol.66, No.3, May 1998, pp.283-301.
18) M. D. Swanson, et al., "Data Hiding for Video-in-Video", Proc. IEEE International Conf. on Image Processing, ICIP-97, Vol.2, pp.676-679.
19) R. B. Wolfgang and E. J. Delp, "A watermark for digital images," Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, Sept. 16-19, 1996, vol. 3, pp. 219-222.
20) Arnold M., "Audio Watermarking", D Dobb's Journal, Vol. 26, Issue 11, pp. 21-26 2001.
21) Arnold M., "Audio Watermarking: Features, Applications and Algorithms". Multimedia and Expo. IEEE international Conf., Vol. 2, 2000 pp. 1013-1016.
22) M.D.Swanson, et al., "Data Hiding for Video-in-Video", Proc. IEEE International Conf. on Image Processing, ICIP-97, Vol.2, pp.676-679.
23) F.Hartung and B.Girod, "Fast Public-Key Watermarking of compressed Video", Proc. IEEE International Conf. on Image Processing, ICIP-97, Vol.1, pp.528-531.
24) F.Hartung and B.Girod, "Digital Watermarking of MPEG-2 coded Video in Bitstream Domain", Proc. IEEE International Conf. on Accoustics, Speech .and Signal Processing, ICASSP-97, Vol.4, pp.2621-2624.
25) F.Hartung and B.Girod , "Watermarking of uncompressed and compressed Video", Signal Processing, Vol.66, No.3, May 1998, pp.283-301.
26) O'Ruanaidh J J K, Dowling W J, Boland F M., "Watermarking digital images for copyright protection" IEE Proceedings-Vision, Image and Signal Processing. 143 (4): 250-256, 1996.
27) Jessica Fridrich, Miroslav Golijan, Rui Du, "Lossless data embedding for all image formats," in Proc. SPIE, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, 2002.
28) Jun Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. Circuts and Systems for Video Technology, vol. 13, no. 8, pp. 890-896, Aug. 2003
29) Adnan M. Alattar, "Reversible watermark using difference expansion of triplets," in Proc. IEEE ICIP, vol. 1, pp. 501-504, Barcelona, Spain, Sep. 2003.
30) Bian Yang, M. Schmucker, W. Funk, C. Busch, and Shenghe Sun, "Integer DCT-based reversible watermarking for images using companding technique," in Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2004.
31) Guorong Xuan, Jidong Chen, Jiang Zhu, Yun Q. Shi, Zhicheng Ni, and Wei Su, "Lossless data hiding based on integer wavelet transform," in Proc. MMSP 2002, St. Thomas, US Virgin Islands, pp. 312-315, Dec., 2002
32) M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in Proc. IEEE ICIP, vol. 2, pp. 157-160, Rochester, USA, Sep., 2002
33) Sunil Lee Chang D. Yoo, Ton Kalker," Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform",
34) Dinu Coltuc and Jean-Marc Chassery "Very Fast Watermarking by Reversible Contrast Mapping", IEEE Signal Processing Letters, Vol. 14, No. 4, April 2007
35) Young-Won Kim, Kyung-Ae Moon, Il-Seok Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics," Seventh International Conference on Document Analysis and Recognition Vol 2, 2003 pp 775.
36) John N. Ellinas, "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection",. World Academy of Science, Engineering and Technology 34 200.
37) M.A.Dorairangaswamy, B.Padhmavathi, "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", IEEE international conference TENCON 2009.
38) Yeung, M. & Minzter, F., "An Invisible Watermarking technique for image verification," Proceeding on the IEEE International Conference on Image Processing, pp: 680-683, 1997.
39) Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dualwrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330,2007

40) W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images", IEEE Transactions on Image Processing, Vol. 8, No. 11, pp. 1534-1548, 1999.
41) Suganya Ranganathan, Ahamed Johnsha Ali, Kathirvel.K & Mohan Kumar, "Combined Text Watermarking", International Journal of Computer Science and Information Technologies, Vol. 1 (5) , 2010, 414-416
42) Mi-Young Kim, "Text Watermarking by Syntactic Analysis", International Conference on Computers, July 23-25, 2008
43) D.Huang and H.Yan. "Inter word distance changes represented by sine waves for watermarking text images", IEEE Transaction. Circuits and systems for video technolo, Vol.11, No.12, pp.1237-1245, Dec 2001.
44) H. M. Meral, E. Sevinc, E. Unkar, B. Sankur, A. S. Ozsoy, T. Gungor, "Syntactic tools for text watermarking", In Proc. of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, 2007
45) M. Atallah, V. Raskin, C. F. Hempelmann, M. Karahan, R. Sion, K. E. Triezenberg, U. Topkara, "Natural language watermarking and tamper proofing", Lecture Notes in Computer Sciences, 2002
46) M. Topkara, U. Topkara, M. J. Atallah, "Words are not enough: sentence level natural language watermarking", In Proc. of 4th ACM International Proceedings of ACM Workshop on ContentProtection and Security 2006
47) U. Topkara, M. Topkara, M. J. Atallah, "The hiding Virtues of Ambiguity: Quantifiably Resilient Watermarking of Natural language Text through Synonym Substitutiions", In Proc. Of ACM Multimedia and Security Conference, 2006
48) W. Bender, D. Gruhl, and A. Lu, Techniques for data hiding, IBM System Journal, 1996, Vol.35(3-4), pp.313-336.
49) X Tang1, Y Niu, H Yue, Z Yin," A Digital Audio Watermark Embedding Algorithm International Journal of Information Technology", Vol. 11 No.12 2005.

Dr. Vipula Singh received her BE degree in electronics from NIT Bhopal And MTech in electronics from NIT Nagpur in 2003 and did PhD in Image Processing from Guru Gobind Singh Indra Prastha University, New Delhi, India in 2009. In 1993, she joined Punjab Communications Ltd.as an R&D engineer. Since 1995 she is in teaching field. Currently she is Professor and Head of department of Electronics and Communication Geethanjali college of engineering Hyderabad India. Her research interests are digital image processing, pattern recognition, artificial neural networks, digital signal processing.