ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 2, No.14 , March 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Recent Digital Watermarking Approaches, Protecting Multimedia Data Ownership

Siddarth Gupta[1], Vagesh Porwal[2]

[1]Department of Computer Science and Engineering, Galgotias University

Greater Noida, Uttar Pradesh 203208, India

siddharthgupta1602@gmail.com

[2]Department of Computer Science and Engineering, Galgotias University

Greater Noida, Uttar Pradesh 203208, India

empower.porwal@gmail.com

Abstract

As the internet networks are proliferating and diversifying across the globe, the accessibility of digital multimedia contents such as images, audios and videos become more frequent. Digital watermarking approaches ensure data authentication, ownership protection and security of digital data. This paper includes of assorted techniques of embedding and extracting watermarks, applied in time-domain/spatial-domain and transform-domain of transmission signal. It imbibes all the ideas of digital watermarking. It starts with the overview, classification, application, possible attacks, limitations, performance analysis and comparative study among various watermarking techniques. Genetic Algorithm approaches are also our primary concern so as to ameliorate each the fidelity and robustness of multimedia data. Audio watermarking is our vital survey area.

Keywords: *Digital Watermarking Schemes, Classification, Frequency Domain Techniques, Genetic Algorithm*

1. Introduction

Dynamic growth of internet connections leads to the vibrant accessing of digital content. Sharing or exchanging of any multimedia data over internet usually disobey the norms of content owner, hence results copyright issues. Actually, the features of digital technology have a critical side effect that lead to easy unauthorized reproduction of information, i.e. data piracy. It is possible to replicate, edit, transmit and distribute the multimedia data and break the intellectual property rights of content ownership. In order to guard the intellectual property rights miscibility, term digital watermarking was first introduced in 1993, once Tirkel showed two watermarking techniques to cover watermark information in images [1].The conception of Watermarking relies on two phenomenon, cryptography and steganography, that manipulate data (messages) so as to cipher or hide their existence [2]. Cryptography and staganography are cousins within the spy craft family: the former scrambles a message thus it cannot be understood; the latter hides the message so it cannot be seen. Except cryptography the conception of watermarking is closely associated with steganography as each hide a message within a digital signal. The key distinction is, watermarking hides a message associated with the actual content of the digital signal, whereas in staganography the digital signal has no reference to the message. In general, watermarking is a methodology for hiding special data (watermark) within cover data so as to save the author possession [3] or we are able to say it's a branch of information hiding that is employed to cover proprietary information in digital media like photographs, digital music, or digital video [4]. Digital signature is also an authentication scheme used to certify the integrity and authenticity of multimedia data. A digital signature [5] is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature, formed by taking the hash of the message and encrypting the message with the creator's private key. The foremost downside [6] of using digital signature is that schemes of it for image authentication encode the signature in an exceedingly file become independent from the initial image, therefore need extra bandwidth to transmit it and also it cannot locate the regions where the digital content has been modified.

The rest of this paper is formulated as follows. Section 2 describes the basic concept of digital watermarking, its principle and classification, basic requirements, radical idea for analysis of various digital watermarking techniques in accordance to different criteria like host signal, robustness, perceptivity, type of watermark, embedding and extraction requirement metrics, processing domain, use of keys, features and applications. Section 3 represents various watermarking techniques applied on digital image as well as on audio, analysis of their embedding and extracting algorithms along with their traits. Section 4 defines the basics of genetic algorithm and its significance. Section 5

illustrates the literature survey of audio watermarking. Section 6 describes possible signal processing attacks. Finally we conclude our whole survey report in section 7.

2. Digital Watermarking Concept

Digital watermarking is basically the process of inserting data into a multimedia element such as an image, audio, or video file. The embedded data (watermark) can later be detected or extracted from the multimedia for diagnosing the copyright owner. Watermark basically symbolizes the person who applied it and, therefore, marks it as being his intellectual property [7]. Evidently, the guarded and unambiguous testimony of the legal owner of any digital content requires that each of individual or organization that develops, owns or transmits digital contents (image/audio/video artists, broadcasting corporations, database providers, etc) adopt a different, unique watermark. The host signal conceal the watermark in it such that it conjoined with the host signal and hence become resistant to any signal z-processing operation without corrupted the host signal. Thus, the digital content (host signal) is still accessible after watermarking but permanently marked. Audio and image authentication are some of the applications of digital watermarking. The objective is to authenticate these digital contents and assure the integrity of the same. Watermarking method is classified in two modules watermark embedding module and watermark detection and extraction module. According [8, 9] to the domain where the owner watermarks are embedded, digital watermarking technologies can be classified into two main groups, i.e. the spatial domain and frequency domain technologies. This paper evaluates the key approaches of digital watermarking and its application in digital image as well as audio copyright protection.
Fig.1 represent general concept of watermarking system [10]. The watermark is encoded in the cover data in the embedding phase. The watermarked object may prone to attack from third party in the transmission phase. The most integral task of the decoder is to retrieve accurate hidden data from the received watermarked image.

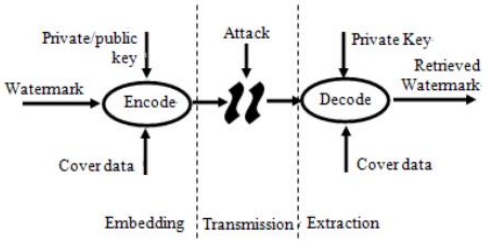

Fig. 1 Watermarking System

2.1 Digital Image Watermarking Approach

Watermarking is essentially the operation of embedding a watermark in a multimedia content i.e., images, video and audio clips or any digital content. Watermark is just a kind of signature that acknowledges the multimedia object owner and has applications like copyright protection, content authentication, tamper detection etc. Watermark may be visible or invisible depending on the applied watermarking algorithm to embed it in a given multimedia object. The embedding operation involves use of a secret key that determine the multimedia object's locations where the watermark would be embedded. Watermark can experience many attacks after its embedding. The attacks may be unintended (low pass filtering or gamma correction or compression) or intended (like cropping). Therefore the watermark needs to be sturdy enough in-tuned of these potential attacks. The sequence of embedded watermark can be extracted by use of the secret key. As the multimedia object might have been attacked or tampered so it is possible that the extracted watermark may or may not simulate the original watermark. Hence to certify the existence of watermark, either *non-blind* watermarking or *blind* watermarking is applied. Former deals with comparing original object and find out the watermark signal while later use a correlation measure to detect the strength of the watermark signal from extracted watermark. The original watermark sequence is compared with the extracted one in correlation based detection. Hence we can determine the existence of the watermark by using a statistical correlation test. The original image and the desired watermark are embedded using one of various currently available schemes. In order to extract the watermark usually a reverse approach is applied to that of embedding stage. In order to forbid illegal access to the watermark a secret key is used during embedding as well as in extraction operation.

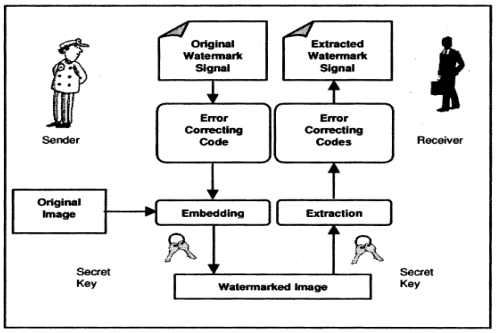

Fig. 2 Watermarking Technique

2.2 Digital Audio Watermarking Approach

The amount of recorded audio data and its anonymous distribution by the Internet, CD

recorders, etc are expanding every day. [11] This results in increase within the illicit recording, copying and distributing of audio files without respect to the copyright of legitimate owners. Audio watermarking techniques provide security from these problems. The basic idea of watermarking is same as delineate above to incorporate a special "code" or data inside the transmitted signal. This code say watermark should be transparent to the user i.e., non-perceptible and robust enough to various removal attacks. Audio signals undergoing the watermarking process should have some desired characteristics:

- Not perceptible (the audio data ought to seem an equivalent to the common attainder before and once the code is embedded).
- Degradation resistant throughout analog channel transmission (i.e. TV, radio and tape).
- Degradation immune to uncompressed-digital media (i.e. CD, digital audiotape and wav files).
- Robust enough to removal through the employment of sub-band coders or psychoacoustic models. (i.e. MPEG, Atrac, etc).

Fig. 3 represents the basic watermarking embedding and detection process using correlation scheme. The watermark embedding process can be represented as: $Y(n) = x(n) + w(n)$, Where $y(n)$ is the watermarked audio signal, $x(n)$ the original signal, and $w(n)$ the watermark signal. We can detect the watermark by correlation that results the decision value of d i.e. $d = d_x + d_w$, Where d_x is intensity of the original signal $x(n)$ and d_w is the energy of the watermark $w(n)$, and expected value of d_x is zero.

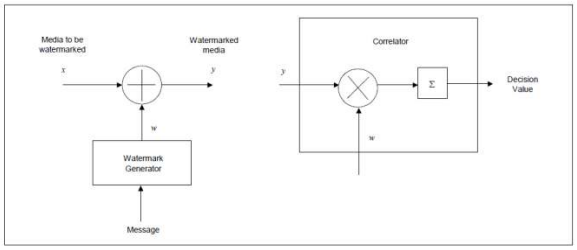

Fig. 3 Basic watermark embedding and detection

Watermarking hides the data in lower frequency components (Fig. 4) of the audio signal shown in, that area unit below the sensory activity threshold of human auditory system [12].

Psychoacoustic Model: Basically the audio watermarking schemes rely on the imperfection of human auditory perceptions [13] so that the embedded watermark is not audible. A psychoacoustic model is a mathematical model used to imitate the human hearing mechanism.

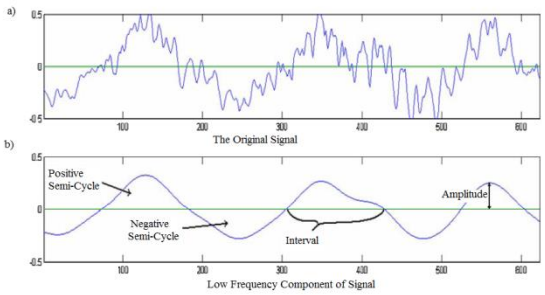

Fig. 4 a) Audio Signal. b) Corresponding Low Frequency Components (LFCs).

Frequency Masking: Frequency Masking is the most integral component of psychoacoustic model that ensures the imperceptibility of the embedded watermark. Frequency masking is the phenomenon where a sound i.e. maskee normally audible becomes inaudible in the presence of a louder sound i.e. masker. The psychoacoustic model estimates the masking threshold via incorporating the frequency masking. So any sound below the masking threshold is inaudible to human ears.

Spread-spectrum: Spread-spectrum modulation method is one of the best watermarking methodology supporting spreading the watermarked signal over the whole spectrum so that it approximates dissonance to be infrasonic (below the ambient noise). A pseudorandom sequence is referred to as chip is used to modulate a carrier wave, produce the signal to spread watermark code.

2.3 Digital Watermarking Requirements

Transparency, robustness, imperceptibility and capacity are four main requirements of digital watermarking.

Transparency or Fidelity: The digital watermark should not alter the quality of the original object after it is watermarked. Cox et al. (2002) outline transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work".

Robustness: Cox et al. (2002) outline robustness as the "ability to discover the watermark after common signal processing operations". Watermarks may well be removed by choice or accidently by simple image processing operations like brightness or contrast improvement, gamma correction etc and audio signal degradation operations like analog channel transmission, sub-band coders or psychoacoustic models. (i.e. MPEG, Atrac, etc). Thus watermarks ought to be sturdy against variety of such attacks.

Imperceptibility: Watermark can neither be seen by human eye nor heard by human ear, solely be detected through dedicated licensed agency.

Capacity or Data payload: Cox et al. (2002) outline capacity or data payload as "the range of bits a watermark encodes inside a unit of time or work". It describes what proportion information ought to be embedded as a watermark to successfully detect throughout extraction.

2.4 Classification

Watermarking process is broadly subdivided into four different aspects in Fig. 5.

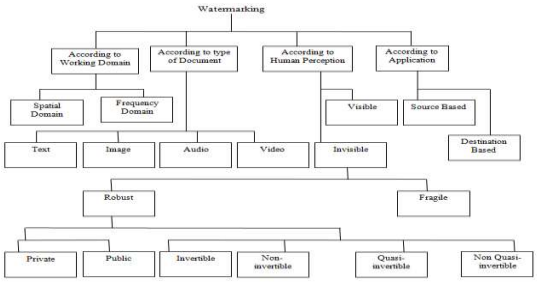

Fig. 5 Classification of watermarking techniques

Basically the classification of watermarking schemes can be organized on the basis of their resistance to host medium modifications [14].

According to perceptivity:

- **Visible:** Visible watermark can be in form of text or a logo identifying the owner. Television channels use visible watermark by superimposing respective logo.
- **Invisible:** Invisible watermarks are embedded into the host signal such that it cannot be detect by human eye. Basically the embedding level is too small to notice and watermark can be retrieved by extraction software. It protects and authenticates the copyright owners well.
  Invisible watermark can also be classified into two types:

1) **Robust Watermark:** A watermark is called robust if it resists a designated class of transformations. Means it aims to embed information in a file that cannot be easily destroyed by any manipulations on it. Robust watermarks have very significant importance in applications where more security is concern.
   It can also be divided into following:

1.1) **Public and Private Watermark:** They are differentiated in accordance with the secrecy needs for the key accustomed insert and retrieve watermarks. If the original multimedia data is not known during detection phase then it is called a public or blind watermark otherwise it is called a private or non blind watermark.

1.2) **Invertible/Noninvertible and Quasi/Non-Quasi Invertible watermark:** Suppose that the copyright owner A embeds his watermark W_A into the host medium I with an inserter E_A [15]. I_A be watermarked image. Let B be any attacker consist of inserter E_B and detector D_B and is able to construct a watermark W_B as well as a fake data I' from I_A such that (1) $E_B(I',W_B)=I_A$, (2)$D_B(I_A,W_B)=1$, (here 1 means "watermarked", and 0 means "not watermarked"), and (3)I' is similar to I_A, then the watermarking system (E_B, D_B) is claimed to be invertible. In Quasi-Invertible watermarking the attacker can find W_B, I', and I_B so that (1)$E_B(I',W_B)=I_B$, (2)$D_B(I_B,W_B)=1$, $D_B(I_A,W_B)=1$, and (3) both I' and I_B are similar to I_A. Quasi-invertible is less flexible than full-invertibility. To overcome such attacks Craver et al. [16] propose a protocol that employs a secure hash, and claim that it is non-invertible.

2) **Fragile/Semi-fragile Watermark:** A watermark is called *fragile* if it fails to be detected after the slightest modification however it is called *semi-fragile* if it resists beginning transformations but fails detection after malignant transformations.

According to type of host signal:

- **Image Watermarking:** The watermark embed into the image as host signal which later on detect and extract in accordance to the copyright ownership.
- **Video Watermarking:** It is basically the extension of image watermarking and adds watermark in the video stream, hence needs real time extraction and strength for compression.
- **Audio Watermarking:** The embedded watermark in audio files should be lower than the perceptual threshold of human auditory system.
- **Text Watermarking:** Hiding watermark in the PDF, DOC and different document to forestall the frequent updates to the text is known as text watermarking.

According to working domain:

- **Spatial Domain:** These methods are based on direct modification of the values of the image pixels hence the watermark needs to be imbedded during this method. Such strategies are easy and computationally economical, so as they modify the colour, luminance or brightness values of digital image pixels hence their application is completed very simply, and requires less computational power. However, the spatial domain watermarking algorithms are generally fragile to signal processing operations or other attacks [17]. LSB technique is one of the oldest spatial domain method, includes

insertion of watermark into the least significant bits (LSB) of pixel data [18].One of the foremost limitation of spatial domain is that the capability of an image to carry the watermark since the effect of modification on pixel values to the cover image, applied by spatial methods like LSB of the data often visually indifferent.

- **Frequency (transform) Domain:** During watermarking in transform domain, the original host data is transformed according to the transform coefficients [19, 20]. These transform coefficients are perturbed slightly in several ways to represent the watermark. Coefficients identification during watermarking is the most severe problem in the frequency domain. Embedding can be done by adding a pseudo-random noise, quantization (threshold) or image (logo) fusion. Most algorithms consider HAS (human auditory system) and HVS (human visual system) for audio as well as image files respectively to minimize perceptibility. The goal is to incur more information bits so that they become robust to attack and are least noticeable. Hence the frequency-domain techniques infix the watermark by restraining the magnitude of coefficients in a transform domain, such as discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT) [21]. We have discussed all these approaches in Section 3. Although frequency-domain methods can yield more embedding information and more robustness against many common attacks, the computational cost is higher than spatial-domain watermarking strategies.

According to type of key:

- **Symmetric or private-key:** In such schemes, both watermark embedding and detection are performed using the same key K.
- **Asymmetric or public-key:** These watermarks can be detected with a key that is different from the one that was used in the embedding stage. A pair of keys is used in this case: a private key to generate the watermark for embedding, and a public one for detection. For each private key, many public keys may be produced.

2.5 Watermarking Applications

The main applications of digital watermarking are discussed as follows:

- **Owner identification and proof of ownership:** In this case the embedded data can carry information about the legal owner of a digital item and be used for notifying/warning a user that the item is copyrighted.

- **Broadcast monitoring:** In this case, the embedded information is utilized for various functions related to digital media (audio, video) broadcasting. The embedded data can be used to verify whether the actual broadcasting of commercials took place as scheduled.

- **Transaction tracking:** In this application, each copy of a digital item that is distributed as part of a transaction bears a different watermark. The aim of this watermark is not only to carry information about the legal owner/ distributor of the digital image but also to mark the specific transaction copy.

- **Usage control:** In usage control application, watermarking plays an active protection role by controlling the terms of use of the digital content. It prohibit unauthorized recording of a digital item (copy control), or playback of unauthorized copies (playback control).

- **Authentication and tamper-proofing:** In this case, the role of watermark is to verify the authenticity and integrity of a digital item for the benefit of either the owner/distributer or the user. Example applications include authentication of surveillance videos, critical documents like passports etc.

3. Watermarking Techniques

Basically there are two main types of watermarks that can be embedded within an image:

- **Pseudo-random Gaussian Sequence:** A Gaussian sequence watermark is an array of numbers including 1 and -1. Hence a watermark constitute of equal number of 1's and -1's. It is also referred as a watermark with zero mean and one variation. We tend to begin by generating q random permutations $\pi_1, \pi_2, \ldots, \pi_q$ of integers between 1 and N. The permutations could be mounted for all images and blocks or modified with the block. Then for each i, $1 \leq i \leq N$, we seed a PRNG We can represent it by an expression that generates a pseudo-random sequence $\xi^{(i)}$ of desired length [22].

$$\xi^{(i)} = PRNG(K \oplus B \oplus i \oplus b_{\pi 1(i)} \oplus b_{\pi 2(i)} \oplus \ldots b_{\pi q(i)}).$$

Within the expression above the symbol $\oplus$ denotes concatenation, K denotes secret key, B denotes block number. The final Gaussian sequence $\eta \in N(0,1)$ is produced by computing $\xi^{(i)}$ for all i and normalizing $\eta = \sqrt{\frac{3}{N}} \sum_{i-1}^{N} \xi^{(i)}$

- **Binary Image or Grey Scale Image Watermarks:** Some watermarking algorithms insert data in form of a logo image rather a pseudo-random Gaussian sequence. Such watermarks are known as binary image or gray scale watermarks. We need a decoder to detect the presence of watermark. Like for pseudo random Gaussian sequence, let W and W' are the original as well as extracted watermark bit sequence, then we can calculate *bit error rate* (BER) to detect the presence of watermark. If BER is zero it means watermark is present otherwise absent. BER can be calculated as follows:

$$D = \begin{cases} 1 \; if \; W_i \neq W_i' \\ 0 \; if \; W_i = W_i' \end{cases} \quad and \quad BER(W, W') = \frac{\sum D}{N}$$

where D is the retrieved signal and N is the number of bits in watermark.

- **Normalized Correlation Coefficient:** It can also be used to detect the watermark.

$$NC(W, W') = \frac{\sum W \, W'}{\sqrt{\sum W_i^2} \sqrt{\sum W_i'^2}}$$

Major frequency domain techniques are as follows:

- **Discrete Cosine Transform (DCT):** It is a sequence of real numbers. It involves conversion of a sequence of data points (spatial domain) to a sum of sine and cosine waveforms with different amplitudes (frequency domain). DCT maps an n-dimensional vector to a set of n coefficients. Zhao et al. [23] encoded a bit of information in a block using the relation between three quantized DCT coefficients (c1, c2. and c3) from this block signifies the middle frequencies. F.S.Wei, X.Feng and L.Mengyuan (2005) embed watermark in DCT domain by changing the phase of five information carriers determined by psychoacoustic model.
  Significance of DCT over other transform applied in watermarking:

1) Watermark is embedded into the coefficients of middle frequency hence the visibility of image will not get affected.
2) Robust to signal processing attacks.

- **Discrete Fourier Transform (DFT):** DFT uses complex numbers rather real numbers and provides a quantitative scenario of the frequency content in terms of magnitude and phase. Solachidis et al [24] deduced a robust watermarking method against rotation and scaling, added watermark directly to the magnitude of the DFT domain.
  Significance of DFT over other transform applied in watermarking:

1) DFT is rotation, scaling and translation (RST) invariant hence, it is robust against geometric distortions.
2) DCT and DWT are not RST invariant.

- **Discrete Wavelet Transform (DWT):** DWT is identical to a hierarchical sub-band system, where the sub-bands are logarithmically spaced in frequency and represent octave-band decomposition. The original image is split into four quadrants contain approximation sub-band (LL), horizontal detail sub-band (LH), vertical detail sub-band (HL) and a diagonal detail sub-band (HH). This process can be applied again and again to produce next coarse scale of wavelet coefficients. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL).Fig.6 below shows the wavelet based transforms:

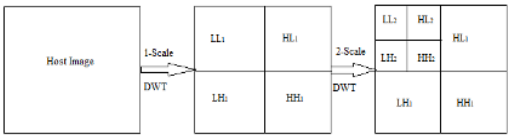

Fig. 6 wavelet transforms

Significance of DWT over other transform applied in watermarking [25]:

1) DWT requires lower computational cost *O(n)* than the DFT or *O(nlog(n))* than DCT, where *n* is the length of the signal.
2) Wavelet process data at different scales / resolutions, shows both large and small features, hence makes watermarking more adaptive.
3) DWT allows very well exploitation of the edges and textures in high frequency sub-band (HH, HL and LH). Hence increase robustness of the watermark added on these large coefficients.

4. Genetic Algorithm

GA is one of the most efficient searching algorithm simulates biological evolution to produce best optimised results [26]. GA is robust, stochastic search methods based on the principles of natural selection and evolution. It starts with some randomly selected genes as the first generation, called *population.* GA can be divided into five segments:

1) **Code:** Any possible solution in problem field is represented by an individual in colony, encoded by a finite-length binary string, called the chromosome.

2) **Original colony:** Randomly selected chromosomes form original colony as the first generation that can reproduce new generation.

3) **Fitness Evaluation:** Evaluate the quality of each chromosome. The chromosome of high quality will survive and form a new population of the next generation. It can be define as the function of imperceptibility and robustness:
fitness = f(imperceptibility, robustness)

4) **Genetic operation:** Selection, crossover and mutation are three key GA operators, applied to the chromosomes repeatedly:

- **Selection:** It is based on tournament selection with both tournament size and probability as parameters to be optimized. It defines the portion of chromosomes with high fitness values survived into next generations.

- **Crossover:** Crossover operator aims at increasing the average quality of the population by swapping genetic information to produce new chromosomes. Crossover needs to be redesigned to keep stable number of 1 bits in each chromosome. The process of crossover is depicted in Fig. 7:

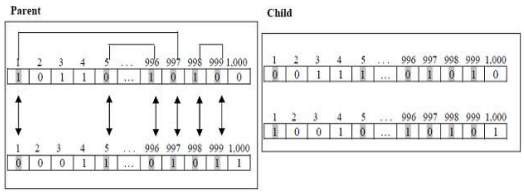

Fig. 7 Crossover

- **Mutation:** It is the occasional random alteration of values in some positions of chromosomes, results expressing new traits from the current generations. The process of mutation uses the reverse operator in order to divide a bit string into sections of size N followed by selection of section and mutated them accordingly.
These operators are used repeatedly to obtain successive generations of chromosomes and aims to the selection of the most-fittest chromosome. They will be passed as parent chromosomes to the next generations.

5) **Terminating rule:** The optimization process terminates when a desired termination criterion is satisfied, like the maximum number of generations is reached, or the fitness value is below a fixed threshold. The fitness value of chromosomes is unchanged after some generations.

- **Significance :**

1) GA helps in the evaluation and selection of more optimised embedding regions during watermarking.
2) Increase the robustness of the watermark contents against various attacks.
3) GA improves the Sim value i.e. the similarity between extracted and original watermark.

5. Literature Summery

In 2005, Wei et al. [27] proposed a blind digital audio watermarking scheme, uses a psychoacoustic model to ensure imperceptibility of the embedded watermark in frequency domain. The psychoacoustic model incorporates the frequency masking phenomenon and estimates the masking threshold. The watermark embed in DCT domain, consists of three stages: pre-processing (6,10 linear clock codes), layer one embedding (symbol embedding) and layer two embedding (bit embedding). Peak point extraction (PPE) scheme is used as a synchronization scheme for achieving blind recovery. Specific regions of watermark embedding are compared with a threshold i.e. sample value of the highest peak after special signal shaping. Extracted peak points are collected via comparing value higher than the threshold. Five phase diverse audio signals are selected to test performance of proposed scheme and shows good robustness against attacks like re-sampling and cropping.

In 2005, Alaryani et al. [28] proposed an audio watermarking technique based on the Low Frequency Components (LFC) of audio signals that do not change much when subjected to common audio signal manipulation. Embedding of watermarks is done by altering the selected samples of amplitude determined by the LFCs of the audio signal. The number of locations reflects the amount of embedded watermarks in the signal. This is basically a blind watermarking approach, independent of the original audio file. The original signal is passed through a Low-Pass Filter (LPF) to extract the LFCs and then determine quartets from the modifiable semi-cycles. The watermarking extraction process is also followed by passing through a Low-Pass Filter to extract LFCs and try to locate all modifiable semi-cycles corresponding to all quartets. The average number of bits of watermarks that can be embedded was found to be 733 bits/file. The decoder in this case is called as "informed detector".

In 2007, Kalantari et al. [29] proposed an audio watermarking scheme based on mean quantization in the wavelet transform domain. The watermark data embeds in the wavelet transform of the original audio signal by quantizing means of two sets of wavelet coefficients, selected from low and high frequency bands. Dither modulation (DM) is used for embedding watermark data in the original audio signal. Since the host audio signal is not required in detection process, the extraction involves use of quantization function and decomposition of each frame of audio signal into four levels, using wavelet transform. The proposed algorithm obtain robustness against many kinds of attacks and shows good performance for well proportioned frequency distribution audio signals.

In 2007, Ketcham et al. [30] proposed an audio watermarking algorithm using DWT-based Genetic Algorithm (GA). GA is applied to evaluate and select the more optimal regions for embedding the binary logo image watermark data. Embedding process followed by transformation of binary logo image into a unidimentional antipodal sequence then decomposition of audio signal into five levels using 4-coefficient Daubecies wavelet (Db4). An object function is defined in order to employ GA into DWT watermarking scheme that is composed of SNR, no of attacking schemes and (Sim) similarity between extracted watermark and original watermark. GA is used to optimize object function and able to search the optimal intensity of watermarks.

In 2008, Bhat et al. [31] proposed an audio watermarking technique using Cepstrum transform-Discrete wavelet transform (CT-DWT), based on BCH coding to hide binary data. It starts by applying code BCH to the watermark data and followed by three consecutive steps of cepstrum transform which are given as: Fourier transform, taking logarithm and inverse Fourier transform. While embedding, the watermark binary image is encrypted using random permutation and is encoded using BCH. The original audio is first segmented into frames and hence transformed into cepstrum domain using cepstrum transform. Watermark is extracted using the db4 filter and decoded using BCH decoding. BCH encoding lowers the bit error rate. This scheme achieves both robustness and inaudibility.

In 2010, Kumsawat et al. [32] proposed a digital audio watermarking scheme. The watermarks are embedded into the low frequency coefficients in discrete multiwavelet transform domain followed by generating a secret key for watermarking, performing pseudo-random permutation to disperse watermark pattern, transforming the original audio signal into five-level decomposition using DMT, selecting the significant coefficients in the DMT domain, embedding the watermark sequence into selected coefficients by quantization index modulation technique and then employs GA to search for optimal quantization steps. The scheme can extract the watermark without the help of the original signal. The optimization technique using GA improve both quality of watermarked audio signal and robustness of watermark

In 2010, Kumsawat et al. [33] proposed a more optimized audio watermarking technique by embedding watermark into low frequency coefficients in discrete multiwavelet transform domain. They employed genetic algorithm to find optimal quantization step during watermark embedding and watermark extracting process in order to maintain integrity of watermarked audio and robustness of watermark. The objective function of GA used for searching process composed of both normalized correlation (NC) and difference (DIF) between desired signal-to-noise ratio (SNR). GA implementation used 20 numbers of chromosomes and binary string as encoding scheme with 32 bit resolution for each chromosome.

In 2013, Chen et al. [34] proposed an adaptive audio watermarking method using wavelet-based entropy (WBE) approach that transforms low-frequency coefficients of discrete wavelet transform (DWT) into the WBE domain followed by calculations of mean values of each audio. Hence it confirms the invariant property for watermarking process. Embedding process includes conversion of synchronization codes into a binary pseudo-random noise sequence and embedded by each audio's WBE mean. The synchronization codes later used to locate positions of embedded watermarks while extraction process. The performance is assessed by the SNR, MOS, embedding capacity, and BER.

In 2013, Lei et al. [35] proposed a robust audio watermarking scheme based on singular value decomposition (SVD) and differential evolution (DE) using dither modulation (DM) quantization algorithm. The watermarking process followed by applying lifting wavelet transform (LWT) DWT to decompose the host signal and obtain the corresponding approximate coefficients followed by DCT.SVD is performed to acquire the singular values and enhance the robustness of the scheme. Synchronization code is inserted as per audio statistical characteristics to handle various attacks. DE optimization resolves conflicts among robustness and imperceptibility effectively, hence attain more robustness among selected attacks compared with previous approaches.

In 2014, Zamani et al. [36] proposed a fragile audio watermarking scheme based on genetic

algorithm to reduce the distortion of LSB substitution, improves the PSNR and increase the payload of the result. The proposed method settles the trade-off among payload and robustness at the same time keeping the quality of watermarking scheme at an acceptance level and hence the substitution technique considerably increased the payload by raising the PSNR that indicates imperceptibility. GA is applied to find optimised embedding coefficients and makes it more robust.

6. Attacks

Following possible attacks are explained in given table [37]:

Table 1: Possible Attacks

Image Compression	Results destruction of an image's watermark
Image Enhancements	Contrast modulation, sharpening
Image Composition	Addition with another image
Information Reduction	Cropping
Geometric Transformations	Translation, Sheering, Rotation of image
Image Filtering	Addition of noise/ blurring
Digital-to-analog conversion	Channel transmission
Forgery	Multiple recipients of different images, all with same watermark

7. Conclusions

In this paper we surveyed the recent literature on digital watermarking approaches in transform domain. We analysed that GA and SVD based audio watermarking process controls the strength of extracted watermark and produce high correlation value, hence increases robustness of watermark as well as host signal against various signal processing attacks. This paper also provides a brief survey on various digital watermarking techniques, applications, requirement metrics, classification and frequency domain techniques.

Acknowledgments

Siddarth Gupta and Vagesh Porwal thanks **Mr. S.P.S.Chauhan**, Assistant Professor, Department of Computer Science & Engineering, Galgotias University for his constant support and guidance throughout the course of whole survey.

References

[1] Van Schyndel, Ron G., Andrew Z. Tirkel, and Charles F. Osborne. "A digital watermark." In Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference, vol. 2, pp. 86-90. IEEE, 1994.

[2] Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." In VISAPP (1), pp. 127-134. 2007.

[3] Kipper, Gregory. Investigator's guide to steganography. crc press, 2004.

[4] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." In Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on, pp. 709-716. IEEE, 2005.

[5] William, Stallings, and William Stallings. Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[6] Chen, Tao, Jingchun Wang, and Yonglei Zhou. "Combined digital signature and digital watermark scheme for image authentication." In Info-tech and Info-net, 2001. Proceedings. ICII 2001-Beijing. 2001 International Conferences on, vol. 5, pp. 78-82. IEEE, 2001.

[7] Nikolaidis, Nikos, and Ioannis Pitas. "Robust image watermarking in the spatial domain." Signal processing 66, no. 3 (1998): 385-403.

[8] Hsu, Chiou-Ting, and Ja-Ling Wu. "Hidden digital watermarks in images."Image Processing, IEEE Transactions on 8, no. 1 (1999): 58-68.

[9] Wong, Ping Wah, and Nasir Memon. "Secret and public key image watermarking schemes for image authentication and ownership verification."Image Processing, IEEE Transactions on 10, no. 10 (2001): 1593-1601.

[10] Song, Chunlin, Sud Sudirman, and Madjid Merabti. "Recent advances and classification of watermarking techniques in digital images." In Proceedings of Post Graduate Network Symposium. 2009.

[11] Garcia, Ricardo A. "Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory." In Audio Engineering Society Convention 107. Audio Engineering Society, 1999.

[12] Hrncar, Martin, and Jan Krajcovic. "Principles of Audio Watermarking."Advances in Electrical and Electronic Engineering 7, no. 1-2 (2011): 247-249.

[13] Wei, Foo Say, Xue Feng, and Li Mengyuan. "A blind audio watermarking scheme using peak point extraction." In Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on, pp. 4409-4412. IEEE, 2005.

[14] Bovik, Alan C. Handbook of image and video processing. Academic press, 2010.

[15] Zhang, Xinpeng, and Shuozhong Wang. "Invertibility attack against watermarking based on forged algorithm and a countermeasure." Pattern recognition letters 25, no. 8 (2004): 967-973.

[16] Craver, Scott, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung. "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications." Selected Areas in Communications, IEEE Journal on 16, no. 4 (1998): 573-586.

[17] Lai, Chih-Chin, Hsiang-Cheh Huang, and Cheng-Chih Tsai. "Image watermarking scheme using singular value decomposition and micro-genetic algorithm." In Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on, pp. 469-472. IEEE, 2008.

[18] Cox, Ingemar, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker.Digital watermarking and steganography. Morgan Kaufmann, 2007.

[19] Asatryan, David, and Naira Asatryan. "Combined spatial and frequency domain watermarking." In Proceedings of the 7th International Conference on Computer Science and Information Technologies, pp. 323-326. 2009.

[20] Mahmoud, Khaled W., Sekharjit Datta, and James A. Flint. "Frequency Domain Watermarking: An Overview." Int. Arab J. Inf. Technol. 2, no. 1 (2005): 33-47..

[21] Barni, Mauro, Franco Bartolini, Alessia De Rosa, and Alessandro Piva. "Optimum decoding and detection of multiplicative watermarks." Signal Processing, IEEE Transactions on 51, no. 4 (2003): 1118-1123.

[22] Fridrich, Jiri. "Robust bit extraction from images." In Multimedia Computing and Systems, 1999. IEEE International Conference on, vol. 2, pp. 536-540. IEEE, 1999.

[23] Zhao, Jian, and Eckhard Koch. "Embedding Robust Labels into Images for Copyright Protection." In KnowRight, pp. 242-251. 1995.

[24] Solachidis, Vassilios, and Ioannis Pitas. "Circularly symmetric watermark embedding in 2-D DFT domain." Image Processing, IEEE Transactions on 10, no. 11 (2001): 1741-1753.

[25] Lumini, Alessandra, and Dario Maio. "A wavelet-based image watermarking scheme." In Information Technology: Coding and Computing, 2000. Proceedings. International Conference on, pp. 122-127. IEEE, 2000.

[26] Yongqiang, Chen, Zhang Yanqing, and Peng Lihua. "A DWT domain image watermarking scheme using genetic algorithm and synergetic neural network." In Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), vol. 2, pp. 298-301. 2009.

[27] Wei, Foo Say, Xue Feng, and Li Mengyuan. "A blind audio watermarking scheme using peak point extraction." In Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on, pp. 4409-4412. IEEE, 2005.

[28] Alaryani, Hamad, and Abdou Youssef. "A novel audio watermarking technique based on low frequency components." In Multimedia, Seventh IEEE International Symposium on, pp. 6-pp. IEEE, 2005.

[29] Kalantari, Nima Khademi, Seyed Mohammad Ahadi, and Amir Kashi. "A robust audio watermarking scheme using mean quantization in the wavelet transform domain." In Signal Processing and Information Technology, 2007 IEEE International Symposium on, pp. 198-201. IEEE, 2007.

[30] Ketcham, M., and S. Vongpradhip. "Intelligent audio watermarking using genetic algorithm in DWT domain." International Journal Of Intelligent Technology 2, no. 2 (2007): 135-140.

[31] Bhat, K., Indranil Sengupta, and Abhijit Das. "Audio watermarking based on BCH coding using CT and DWT." In Information Technology, 2008. ICIT'08. International Conference on, pp. 49-50. IEEE, 2008.

[32] Kumsawat, Prayoth. "An efficient digital audio watermarking scheme based on genetic algorithm." In Communications and Information Technologies (ISCIT), 2010 International Symposium on, pp. 481-485. IEEE, 2010.

[33] Kumsawat, Prayoth, Kitti Attakitmongcol, and Arthit Srikaew. "Genetic algorithm optimization of multiwavelet-based audio watermarking." InProceedings of the 9th WSEAS international conference on Applications of electrical engineering, pp. 111-116. World Scientific and Engineering Academy and Society (WSEAS), 2010.

[34] Chen, Shuo-Tsung, Huang-Nan Huang, Chur-Jen Chen, Kuo-Kun Tseng, and Shu-Yi Tu. "Adaptive audio watermarking via the optimization point of view on the wavelet-based entropy." Digital Signal Processing 23, no. 3 (2013): 971-980.

[35] Lei, Baiying, Yann Soon, and Ee-Leng Tan. "Robust SVD-based audio watermarking scheme with differential evolution optimization." Audio, Speech, and Language Processing, IEEE Transactions on 21, no. 11 (2013): 2368-2378.

[36] Zamani, Mazdak, and Azizah Bt Abdul Manaf. "Genetic algorithm for fragile audio watermarking." Telecommunication Systems (2014): 1-14.

[37] McCloskey, Scott. "Hiding Information in Images: An Overview of Watermarking." Cryptography Research Paper (2000): 11-9.

First Author Siddarth Gupta has done B.tech in CSE from UPTU, Lucknow, Uttar Pradesh, India in 2012. Currently he is pursuing M.tech in CSE from Galgotias University, Greater Noida, Uttar Pradesh, India. He is working on project "Robust Digital Image/Audio Watermarking in Frequency Domain".

Second Author Vagesh Porwal has done BCA from IGNOU, Raebareli, Uttar Pradesh, India in 2011 and M.Sc from MDU, Rohtak, Haryana, India in 2013. He is currently pursuing M.tech in CSE from Galgotias University, Greater Noida, Uttar Pradesh, India.