CHAPTER-II  
 
LITERATURE REVIEW

The main subject of the literature is to provide the base for the evaluation of the proposed ideas. This part of the project is divided into two main parts, one is the back ground knowledge and the requirements of watermarking, the second part is the state of art of watermarking system.

The chapter is further divided as follows. Describes a generic watermark model which is the basis of all watermarking system in section-2.1. The properties of digital watermarking are discussed in section-2.2. The issues of robust watermarking are described in section-2.3. The issues of fragile watermarking are discussed in section-2.4.

2.1. WATERMARKING OF DIGITIAL IMAGE

The Code-breakers [41], D. Kahn recounts in their wonderful book, one of the stories in the Histories of Herodotus in which Histiaeus tattooed a message in the shaven head of a slave and waited for the new hair to grow before sending him to Aristagoras at Miletus with instructions to shave-again-the slave’s head. Though, the state-of-art in Digital Watermarking was not very difficult in earlier days but there is not much change in the method.
Useful information pertaining to the content creator or owner is hidden by Digital Watermarking for data copyright and authentication purpose[24]. Steganography was a more former Watermarking name. This word has its origin in Greek. “Stegano” means “covered” and “graphos” means “to write” [60, 74]. Together steganography means literally “cover writing”. This term, steganography, is not yet popular in literature. Digital watermarking is used by most people, information hiding and data embedding. Among them, watermarking is most recognized by general public and is by far, popularly used in commercial products.

More specifically, digital watermarking, also called watermarking embedding or watermark insertion, where the hidden information is inserted into multimedia data also called cover media. The hidden information which is also referred to as watermark, may be random number sequence or the serial number (usually based on some distribution, such as uniform or Gaussian), ownership identifier, text, creator of work, copyright messages, gray or binary level image etc. After the watermark is embedded, the original cover media will be the modified content and slightly modified is called watermarked content.
The figure-2.1 shows a typical watermarking system in which there is fixing of watermark and its extractor. The inputs to the watermark embedded are watermark, the secret key and the cover content. The security of watermarking system is enhanced by this secret key. The output of the watermarking embedded is the watermarked content. Depending on the method, the original cover content or the watermark, the input to the watermark extractor are the watermarked content, the secret key (at the time of embedding same as used). As discussed in [24], a watermark detector involves process of two steps. The first step is extraction of watermark that applies one or more pre-process to extract a vector called as extracted watermark. Then the second step is to determine whether the extracted watermark is same as watermark of original or not. The comparison of the watermark extracted with the original also called reference watermark and result could be some kind of confidence measurement indicating how likely the watermark of original is present in the content is involved in this process usually[37]. Other media can replace the multimedia content shown in Figure-2.1. The commonly applied media are 3D data [10,11,82], audio [75], image [23], text [14], and object [73], video [33].
Now suppose that $X$ is the cover content, $W$ is the watermark and $k$ is the secret key. In watermarking system an embedding function $P(.)$ takes $X$, $W$, and $k$ as input parameters and outputs the watermarked content, say $X^0$ as:

$$X^0 = P(X, W, k)$$

If they are fixed firmly in such a way that watermark survives even if the watermark content $X^0$ goes through severe attacks, the watermark is considered as robust. The extraction of watermark procedure is explained as follows:

$$W^0 = Q(X^0, k, [X], [W])$$
Where, $Q(.)$ is the extraction function. $X$ and $W$ enclosed in braces $'[]'$ can be optional inputs of extraction function. For example $[X]$ can be used when the watermarking system should not be blind. That is the watermarking system under consideration requires the True image for the extraction of the watermark.

Several requirements must be satisfied for typical watermarking system [93].

- They extract the watermark $W^0$ from $X^0$ with or without the $X$

- $X^0$ should be as close to $X$ as possible in most cases.

- If $X^0$ is unmodified, the detected watermark $W^0$ should be exactly same as $W$

- If $X^0$ is modified, $W^0$ should still match $W$ well to give clear judgment of the watermark existence for robust watermarking.

- $W^0$ will totally be different from $W$ after even the slight modification to $X^0$. $W^0$ can point the possible tampering to $X^0$ and give information about the degradation of $X^0$ for fragile watermarking.
2.2. DIGITAL WATERMARKING PROPERTIES

To have an effective digital watermarking, it must have number of properties. We explain these properties as below:

2.2.1. Imperceptibility

It is generally required to have watermarked image which should perceptually be as close to True image as possible. Otherwise, its aesthetic value would be degraded, the distortions caused by watermarking embedding process. This property is called transparency or imperceptibility of the watermarking system[89]. If a system of watermarking destroys the cover image till it become useless, the watermarking system has very little use. Theoretically, even on the highest quality equipment the watermark should be invisible to human eye[43].

To maintain the imperceptibility either Human Visual System or Just Noticeable Difference models are used during the watermark embedding. The Just Noticeable Difference is maximum allowable modification in signal such that modified signal is not distinguishable by human being. Watson et al. [85] proposes the JND model in wavelet domain. It is specified by HVS that visual system of human eyes has certain characteristics. The eyes are less sensitive to changes made in highly
textured regions compared to flat regions. The textured regions have complex patterns whereas the flat regions are monotonous. A bigger watermarking weight can be used in an additive embedding for the image regions that have complex textures using HVS compared to those regions with simple textures.

For the evaluation of the generally, imperceptibility, Peak Signal to Noise Ratio is used. The PSNR is the least mean square errors between images of original and watermarked. According to some researchers PNSR is not perfect metric to measure the imperceptibility[89,91].

2.2.2. Robustness

By Robustness in the watermarking system it means the capability of watermark to survive against both legitimate and illegitimate attacks. Which does not particularly aim at removing the marking or watermark it unusable are the Legitimate or unintentional attacks. The attacks particularly aim at damaging the fixed watermark in the cover work[6, 55] are illegitimate or intentional attacks. Except in fragile watermarking systems, almost all watermarking systems required need to be resistant against any illegitimate or legitimate of watermarked image processing. These attacks and their counter measures are studied in the context of
the watermark applications, as different approaches are mostly concerned with a different set of conceivable attacks[15]. Therefore, the system of watermarking intended application and thus corresponding set of conceivable attacks are of prime importance while designing it[24].

To have digital image watermarking, the watermarking algorithm should generally be very robust to sustain for any type of damages like noise addition, scaling, translation, geometrical transformations such as rotation, and lossy compression such as JPEG compression[93].

2.2.3. Capacity

Regarding capacity of the watermarking system, it is defined as the maximum amount of information that could be affixed firmly in the cover work for which some technique could be profitably used[6]. There is always tradeoff between capacity and other two important watermarking system properties are robustness and imperceptibility. A higher capacity is always obtained by sacrificing either imperceptibility or robustness (or both), it is thereby necessary that a good tradeoff is found depending on the application on hand[6].
2.2.4. Detection of Blind or Non-blind

The image is called blind when watermarking technique does not require original image to recover the watermark from the watermarked images. Alternatively, if the watermarking technique need original image to take out the watermark from the watermarked image, it is said to be non blind. The blind images are called oblivious. The non-blind watermarking are more robust than blind watermarking because of availability of original cover image at the time of detection. The blind or oblivious watermarking systems are more popular. Oblivious watermarking systems are more popular. Oblivious watermarking system reduces the cost of overhead and memory for storing original images.

2.2.5. Security

If hackers want to hack it is not possible became he must have total knowledge of embedding algorithm, composition and detector of watermark, it is said to be secure. A secure watermarking system can resist many hostile attacks which thwart the watermark’s purpose[24]. The attacks that can embed, remove, detect or modify the watermark are illegal operations. Unauthorized embedding or removal is referred as active attacks while detection of unauthorized detection is termed as passive attacks.
2.2.6. The Cost of Computation

A watermarking method should be less complex in order to reduce computational cost. More sophisticated hardware’s and software’s recourses are required to compute the cost of computation. In resource-limited environments like mobile devices the computational simplicity is usually preferred. A balance between memory allocation, bandwidth usage, battery power consumption and many other factors have to be found in mobile devices current applications. Similarly, in case of telemedicine, the cost of bandwidth consumption when medical images are exchanged through networks, located to remote hospitals in rural areas of country can be cut by computationally less expensive algorithms.

2.3. WATERMARKING SYSTEMS OF ROBUST

Against wide range of unintentional and intentional image processing operations such as image filtering, enhancement, JPEG compression, noise addition, collusion, geometrical transformations, and forgery attacks[24, 23, 62, 50], a robust watermarking system is resilient.

2.3.1. Attacks on Robust Watermarks

To perform attacks on the toughness of the watermarking systems can be made possible by the availability of wide range of unique processing
software’s. The objective of these attacks is to protect the watermark from performing its intended purpose. The common attacks performed on watermark robustness are explained as given below:

2.3.1.1. Degradation of image

The robust watermarks are damaged by these types of attacks by removing parts of the image. The watermark information may be carried by the parts that are replaced. Examples of these operations are row removal, partial cropping, and column removal. Insertion of Gaussian noise also comes under this category, in which the image is degraded by adding noise controlled by its variance and it’s mean.

2.3.1.2. Enhancement of image

The watermark information in an image is desynchronized by these attacks that are convolution operations. These attacks include sharpening, histogram, smoothing, equalization, contrast enhancement and median filtering.

2.3.1.3. Compression of image

Images are generally zipped with JPEG2000 and JPEG compression techniques in order to minimize storage space and cut the cost of
bandwidth required for transmitting images. These lossy compression methods are more damageable as compared to lossless compression methods. The watermark information with inverse operation can be recovered by lossless compression methods. However, irreversible changes to the images are produced by lossy compression techniques. Therefore probability of recovering watermarked information is always very low.

2.3.1.4. Transformations of image

Stir Mark[60,61], used the software for small local geometrical distortions to invalidate watermark detection. These types of attacks are also called geometrical attacks or synchronization attacks. Geometrical attacks include translation, scaling and rotation also called RST attacks. Some researchers focus on RST robustness while designing the robust watermarking systems, because it is fundamental problem. Besides RST transforms, other transforms such as shearing, aspect ratio change, projection and reflection are included in image transformations.

2.3.2. Robust Watermarking Applications

In number of applications, robust watermarking systems have been proposed to be implemented. Some major applications are described here under:
2.3.2.1. Copyright protection

The copyright protection is one of the major applications of robust watermarking. The idea is the embedment of information regarding the copyright owner into the content to preventing the parties from claiming to be the rightful owners of the data. Despite common image processing manipulations, the robust watermark embedded into the content is detectable. Therefore, the deliberate removal of the robust watermark would results in severe degradation of the image’s visual appearance. The owner can be identified positively by the successful detection of the watermark.

2.3.2.2. Fingerprinting

The features of an object that tend to differentiate it from other small objects are Fingerprints. As per in the applications of copyright protection, the watermark for finger printing can be utilized to trace authorized users who right the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer’s identification number.
2.3.2.3. Access control

The users are entitled to have different privilege (copy/play control) on the object by different payment. In some systems, to get a copy and usage control mechanism to restrict the limit the number of times of copying or illegal copy of the content is desirable. They can use a robust watermark for such purpose[93]. Bloom[12] et al. applied the robust watermark to the access control and copy protection of DVD.

2.3.3. Various Styles of Robust Watermark

Till data only few of the different styles of robust watermark have been reported, the literatures of whom are described below:

2.3.3.1. Noise Watermark

The very generally used type of robust watermark is Noise watermark. It is demonstrated that the watermark is most secure, if it is in the form of Gaussian random sequence for the reason of security and statistical undetectivity. The correlation value is used to indicate the similarity to measure the similarity between extracted and original sequence.
2.3.3.2. Logo Watermark

Logo is another form of robust watermark. The logo is small image pattern in binary form. It can be company logo used in business or commercial purpose applications. The quality of logo image is measured by human perception. That is, it is subjective measure of verifying authenticity of the digital content.

2.3.3.3. Message watermark

Message watermark comprises text and has the advantage of easy to use in comparison with logo watermark or noise-type watermark. However, bit error rate approaching to zero is required in the message watermark, because any bit error will cause major fault in the final output. In most cases it is need that information with at least 64 (or 8 ASCII character can be carried by multimedia) bit.

2.3.4. Methods of Robust Watermarking

2.3.4.1. Robust watermarking based on spread spectrum

Cox [23] et al. introduced Spread spectrum watermarking. The information is embedded by the spread spectrum communication using small amount of energy with large spectrum. The corresponding energy or information become very small and undetectable in each band. Thus, the
removal of the signal (watermark) from the host signal (cover content), if spread spectrum communication is applied is difficult.

Cox [27] et al. approach uses spread spectrum communication techniques embed a single bit in the image.

Pickholtz [63] et al. defined spread spectrum communication as: “Spread spectrum is a means of transmission in which the signal occupies a band width in excess of minimum necessary to send the information, the band spread is accompanied by a code which is independent of the data, and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery”.

2.3.4.2. Robust watermarking based on JND model

Wolfgang [88] et al. proposed to embed the amount of modification on image which will not be aware by human perception as Just Noticeable distortion. Their model was tested in both DWT and DCT domains and the output indicated that the manipulation is not noticed by human eyes. HVS or JND model are subjective measure of transparency.
Delaigle [25] et al. discussed the masking effect, the minimum level below which a signal can’t be aware, in Discrete Cosine Transform domain. The watermark can be embedded into an image in a manner such that human eyes can’t perceive using the masking effect.

Barni [7] et al. perform robust watermarking by applying the masking effect of human perception in embed pseudo random sequence as watermark and Discrete Cosine Transform domain

2.3.4.3. Robust watermarking based on spatial domain

Nikolaidis [58] et al. proposed robust watermarking in spatial domain. Random selected pixels are modified by the authors and use hypothesis testing to detect the watermark. It is claimed by them that their approach is robust to low pass filtering and JPEG compression.

2.3.4.4. Robust watermarking based on channel state estimation

Voloshynovisky [80] et al. explained the scenario of optimal embedding and extraction of watermark. The watermark problem was treated by them as communication with side information. Attacks including noise, geometrical attack and fading are taken into consideration in their scenario. The side information proposed in their paper includes secret
key and channel state information such as cover image and attack channel. According to the combination of whether the side information is available on watermark embedding and watermark extraction. It was concluded by them that the optimal watermarking system should take all available side information into consideration at both extraction and embedding of watermark.

2.4. FRAGILE WATERMARKING

It is very easy to destroy watermark. This idea is very useful to identify whether a multimedia is modified or not. The authenticity of multimedia can be authenticated by modulating fragile watermark into multimedia. The corresponding embedded fragile watermark will be made destroyed if any modifications on the multimedia are there. The position where the modification occurred can be identified easily by examining a fragile watermark.

2.4.1. Authentication of document

The document authentication is very important in commercial applications. Images, texts, tables and logos are included in the contents of a general document. Thus, for the protection of document, a more number of authentication techniques could be used.
2.4.2. Authentication of Evidence

The next approach of the fragile watermark is the proof of authentication in the court of law. Video or image of crime or violation of law can be utilized as proof so to say as evidence in the court of law. The authentication of evidence should be proved ultimately.

2.4.3. Complete Authentication

The integrity of the entire multimedia is checked by Complete Authentication. A simple way is to use a hashing function to compute a signature and use this signature to perform authentication to authenticate the content. Any modification change on the content will cause change of the signature, thus we can detect the modification. Any bit error will make the contents treated as being tampered with in application of complete authentication. Even though use of multimedia is a lossy approach but commonly multimedia is only under use because it gives the complete authentication. Hence, the only lossless compression can be utilized. Another demerit of complete authentication is that we only get aware about the occurrence or non-occurrence of modification. The status of where the modification occurred is still unknown.
2.4.4. Authentication of Content without Incidental Distortions

Content authentication not only responds about the modification of multimedia is done or not but also represents where the tampering has been made in comparison with complete authentication. The approaches that are used for this type of authentication are as follows:

2.4.4.1. Fragile watermark based on quantization

Kundur and Hatzinakos[46] recognizes the types of incidental distortion as JPEG compression, if the ratio of the number of destroyed watermark against the number of all watermark gets minimized form high resolution to low resolution in wavelet transform. However, the type of modification can’t be identified their approach if both an instance of malicious tampering and incidental distortion are applied simultaneously.

2.4.4.2. Block hashing

Wolfgang and Delp [87], had compared two methods to perform image authentication. Hash function is generally applied on blocks of image in the first approach. Any modification on this protected image varies the value of the hash function. Hence, area which is tampered with can be identified. They examined the VW2D in next approach. The stored
values obtained watermark is utilized by the VW2D technique and the watermarked image to execute image authentication on a block-by-block basis. These two examined methods need store values for immediate processing. An extra need of management of these stored data is required.

2.4.5. Authentication of Content Distinguishing Incidental Distortions

Lossy compressions are commonly used in order to reduce the amount of data in multimedia. Hence, lossy compression must be treated as incidental distortion. The identification of the area that is maliciously tampered is the objective of multimedia authentication. Thus, a useful authentication should be able to differentiate an instance of malicious tampering from an incidental distortions. The compression, blur and sharpening are the examples of the incidental distortion. The watermark which can resist incidental distortion and gets destroyed by malicious tampering is called semi-fragile watermark. The approaches used for this type of authentication are as following:

2.4.5.1. Digital signature

Lin and Chang [51] have proposed a digital signature-based method to perform JPEG compression tolerated image authentication system. The local integrity of DCT block as signature is recorded by the
digital signature approach and this signature is used for content authentication. If the local integrity does not get changed by compression operation which will be destroyed by other operation, then the incidental distortion and malicious tampering on multimedia will be differentiated. The merit of digital signature approach is that compression can be tolerated by this method with any ratio. But the demerit is that extra storage space is need required to store the “digital signature”.

2.4.5.2. Feature points

Bhattacharjee and Kutter [8] proposed to use encrypted digital signature of feature point of image to perform compression tolerant image authentication. Since most image processing operations can be tolerated by feature point, the feature points are still authenticated if the position and number of feature points remain unchanged. Otherwise, if the image is maliciously tampered with, then the position and number of feature position will be changed as well. Under the circumstances, where the modification occurred can be identified. However, the feature point-based approach is still not reliable. Some feature point may be lost, and the error response is then occurred by applying image.

CHAPTER-III