Sheikh Imran al. International Journal of Recent Research Aspects ISSN: 2349-7688, Special Issue: Engineering Research Aspects Feb 2015, pp. 74-78

The Techniques and Applications of Digital Watermarking

Sheikh Imran[1], Ravinder Chaudhry[2], Junaid Gilani[3], Suhail Nehvi[4]

[1]Student, M. Tech, ESEAR, Ambala
[2]Assistant Professor, Dept. of EE, E-Max group of Institutions, Ambala
[3]Head, Department of Electronics and Communication, J&K Technical Education.
[4]Lecturer, Govt. Polytechnic for Women, Srinagar.

Abstract---- **Digital Watermarking is an emerging field that aims to extend the benefits of authentication and copyright to the digital media. These Watermarks remain hidden and do not degrade the quality of the digital media. Different techniques are used for incorporating watermarks into the media. Similar techniques are used at the receiver to retrieve watermarks. However, watermarks are susceptible to attacks, and robustness, which quantifies the resilience to attacks, is an important property for all watermarks. However, in most cases, it is the application, for which the watermarking is used, that dictates the features that watermark should possess. In this paper we have elucidated the techniques and applications of digital watermarking.**

Keyword: Digit Watermarking, Image, digital media.

I. INTRODUCTION

The digital media has become increasingly popular in the recent times owing to its advantages in terms of easy storage, duplication and distribution in comparison to analog media.

The digital watermarking is a technique used to safeguard the copyright of digital media by hiding certain information in the original data. The hidden information can be retrieved at any time by the owner of the data to prove his ownership [1]. The information inserted into the media can either be a meaningful entity like a logo, a trademark etc or even a meaningless sequence of digital bits [2]. Once the digital media is transferred over the channels of communication, it may undergo intentional or unintentional modifications [3]. These are called attacks. Most of the attacks are malicious attacks that aim to remove the original watermark from the digital media thereby creating doubts about its ownership [4]. Therefore, watermarking should be robust to withstand any such attacks [5, 16] .Other issues related to watermarking include perceptibility and capacity. The perceptibility of the watermark means that the original media, usually an image, should remain the same as seen by naked eye, after hiding the watermark in the media. Capacity refers to the amount of payload or the maximum number of bits of watermark information that can be accommodated in the digital media without degrading its perceptibility. A tradeoff is usually made between robustness, perceptibility and capacity depending upon the application where the watermarking is to be used. The watermark itself could be introduced as a fragile watermark. A fragile watermark is different from robust watermark, in which the slightest modification of the original media will destroy the watermark. This instantly detects any tampering.

In most cases a watermark does not necessarily have to possess all the characteristics. On the contrary watermark has those properties which are specific to a particular application. In short it is the application that dictates the features that a watermark should have.

Techniques of Digital Watermarking

Digital watermarking is similar to the task of electronic communication as there are well defined stages of generation, transmission and reception [5].

Watermarks are first generated and embedded into a digital media. Then this watermarked media is distributed over some channels (e.g. internet) which can be both lossy and susceptible to attacks. Once a watermarked media is received, watermark can be retrieved for verifying its authenticity or authorship. We discuss each of the stages below.

Watermark generation and embedding.

Generation is very critical stage of the watermarking process. The requirements of watermark generation are uniqueness and complexity. Watermarks contain information that must be unique. Otherwise the owner cannot be uniquely identified [6]. Watermark signals are characterized with a great complexity. This is necessary in order to avoid the construction of similar watermarks. Subsequently, watermark determination by a third

person becomes more difficult. Another advantage of complex watermarks is that they provide reliable statistical properties and their detection can be shown with great certainty [7] [8] . There are two kinds of watermarks viz: meaningless watermarks and meaningful watermarks.

II. MEANINGLESS WATERMARKS

a.) Pseudo random sequence.

It is generated by a seed which is the watermark secret key. The pseudo random sequence is used as watermark signal which is a normal distributed sequence having zero mean and variance, unity. The most frequently used pseudo random sequence is the binary random sequence called as M - Sequence which is generated by linear shift register.

M sequence is a binary pseudo random sequence and is more often than not used as watermark. It can be embedded as the watermark directly or it can be used as the separate sequence for the watermark signal.

b). Chaotic sequence.

Due to the advantages such as easy implementation, secured security, chaotic sequence is sometimes used as the watermark, especially the Bernoulli chaotic sequence.

III. MEANINGFUL WATERMARKS

Meaningful watermarks can be in the form of texts, audio, image or video. No matter what form it is, most of the meaningful watermarks are converted into binary sequence before they are embedded. Here are some examples of them:

a) Spread spectrum sequence

By making the use of M sequence, we can make our meaningful watermarks as a spread spectrum sequence, e.g. According to the value of the watermark signal (0 or 1), we can embed the identical M-sequence or inversed M sequence.

b) Bit plane decomposition

This method for gray level images can decompose them into eight bit planes b0, b1, …..b7, in the order from least significant bit to most significant bit with the value 1 or 0 for each. For color watermark signal, it can be represented in RGB first and then we can do the decomposition as the gray- scale watermarks.

c) Permutation of watermarks

Permutation can be used in the pre processing of watermarks to secure the watermarking system.

Watermark embedding can be performed in a variety of ways [9]. There are two main groups of watermark embedding technologies: coefficient- based and system based. Coefficient based approaches are the most obvious approaches since the embedding process is performed by a direct modification of a pixel values or transform coefficient values. Examples of this group are approached based on pixel modifications in the spatial domain, such as least significant bit watermarking where the least significant bit of the pixel values are replaced by the binary watermark values. Extensions of this basic idea are, for example, based on spread spectrum communication and can be applied to a variety of domains, such as the frequency domain and wavelet domain. The second group is less obvious to understand because the watermark embedding process is performed by slightly changing an existing processing system. One example of this group is fractal image watermarking.

Depending upon the domain where the embedding is performed, it can be divided into spatial domain based watermarking and transform domain based watermarking.

Spatial domain: Spatial domain digital watermarking algorithms directly load the raw data into the original image [10]. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Techniques are based on direct manipulation of pixels in an image [11]. Some of its main algorithms are as discussed below:

Additive Watermarking: The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low [12].

Least Significant Bit: This is an old popular technique that embeds the watermark in the LSB of pixels. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image.

Spread Spectrum Modulation Based Technique: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

Patchwork Algorithm: Patchwork is a data hiding technique developed by Bender et al and published on IBM Systems Journal, [13]. It is based on a pseudorandom, statistical model. Patchwork

imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened whereas that of patch B is darkened.

Correlation-Based Technique: In this technique, a pseudorandom noise (PN) pattern say W(x, y) is added to cover image I(x, y). Iw(x, y) = I(x, y) + k*W(x, y), where k represent the gain factor, Iw represent watermarked image at position x, y and I represent cover image.

Transform domain: The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients [14].

Discrete cosine transform (DCT): DCT represents data in terms of frequency space rather than an amplitude space. This is useful because it corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking.

Discrete wavelet transforms (DWT): The transforms are based on small waves, called wavelets, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely.

Discrete Fourier transform (DFT): This transforms a continuous function into its frequency components. When used with images it is resolved in into different frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance.

Distribution and possible attacks:

Once the watermarks are embedded, the digital media can undergo various processes over open channels, just as in the case in a communication medium. The digital media can be subjected to both unintentional and intentional changes. The unintentional changes include compression, cropping, resizing and filtering of a digital image. The intentional attacks are mostly malicious aimed at removing the watermark from the media. Robust watermark must be resistant to both unintentional and intentional attacks. The attacks can be further classified as follows:

Simple attacks:

Simple attacks are conceptually simple [15] [16], which always contain some normal manipulations of image.

Removal attacks are attacks that attempt to separate the watermark signal and cover image and then delete the watermark signal from the cover image.

Geometrical attacks:

Geometrical attacks are the attacks attempting to destroy the synchronization of detection, thus make the detection impossible. All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

Ambiguity or protocol attacks: The protocol attacks neither aim at destroying the embedded information nor do they disable the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermarks implementation.

Copy attacks: The copy attack is aimed to form an estimate of the watermark and then use the same to watermark another image.

Detection of watermark:

Detection is a crucial part in the watermarking framework. It allows the owner to be identified and provides information to the intended recipient. There are two kinds of detection: Informed Detection and Blind detection according to whether the original image is needed or not in detection. For informed detection which means the original image is used in detection, the watermarking system is called private watermarking. For blind detection which does not need the original image, the watermarking system is called public watermarking. According to different applications, different systems are applied, e.g. for authentication, it is impossible to obtain the original image in the detection. Also for some very confidential application, it is better to use the private system. Depending on the way the watermark is inserted and the nature of the watermarking algorithm, the detection or extraction method can take on very distinct approaches. Generally speaking, we can divide them into two groups: the inverse process or the correlation peak calculation [17]. Many detection methods use the exact inverse process of embedding to get the watermarks. For those systems which take the pseudo random noise or sequence as the watermarks, the correlation can be computed to decide whether there is watermark or not. The receiver side uses the same key used in embedding process to generate a pseudo random sequence and then computes the correlation between the new generated

sequence and the received data. If the correlation value can arrive at a peak which is over a threshold, we can claim that watermark is detected, otherwise, it is un-watermarked.

IV. DIGITALWATERMARKING APPLICATIONS

Digital watermarking can be useful in several areas of interest involving digital images[4]. In order to fully understand the challenges involved in the development of watermarking-related tools, some applications of watermarks are listed below.

Copyright protection: Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

Tamper proofing*:* Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

Copy protection: Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content [18].

Broadcast monitoring: Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters

Fingerprinting: In order to trace the source of illegal copies, the owner can embed different watermarking keys in the copies that are supplied to different customers. For the owner, embedding a unique serial number-like watermark is a good way to detect customers who break their license agreement by copying the protected data and supplying it to a third party.

Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [17].

Annotation and privacy control: Multi-bit watermarking can be used to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other usages of annotation watermarking are electronic `document indexing and automated information retrieval.

V. REFERENCES

[1]. Su, J.K., F. Hartung, and B. Girad, Digital Watermarking of Text, Image and video Documents. 1991, University of Eriangen-Nuremberg: Erlangen.

[2]. Barni, M., et al,. Watermark embedding: hiding a signal within a cover. Communications Magazine. IEEE, 2001. 39(8): p. 102-108.

[3]. Duric, Z., N.F. Johnson, and S. Jajodia, Recovering Watermarks From Images. 1999, George Mason University.

[4]. Ensaf Hussein, Mohamed A. Belal, ,Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey, IJERT, ISSN: 2278-0118, Vol. 1 Issue 7, September-2012

[5]. Miyaziki, A. And A. Okamoto, Analysis And Improvement of Correlation- Based Watermarking Methods For Digital Images. 2002, Kyushu University.

[6]. Bruce, A.M., A Review of Digital Watermarking. 2001, University of Aberdeen.

[7]. Delannay, D. and b. Macq, Gemeralized 2-D Cyclic patterns For Secret Watermark Generation: Belgium.

[8]. Research on Digital Watermarking At Aristotle University of Thessaloniki. 97, Aristotle University of Thessaloniki, Korean: Korean.

[9]. F. Hartung and M. Kutter, " Multimedia Watermarking Techniques." Proc. IEEE, Special Issues on Identification and Protection of Multimedia Information, Vol. 87, no. 7, July. 1999, pp. 1079-107

[10]. Jiang Xuehua, -Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[11]. Literature Review, Source: Internet

[12]. http://ippr-practical.blogspot.in

[13]. Manpreet kaur, Sonia Jindal, Sunny Behal, A Study of Digital image watermarking, Volume2, Issue 2, Feb 2012.

[14]. Voloshynovskiy, S., et al., Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. Communication Magazine, IEEE, 2001. 39(8): p. 118-126

[15]. Mohanty, S.P., K.R. Ramakrishnan, and M. Kankanhalli, A Dual Watermarking Technique for

image, quoted by jian Liu and Xiangjian He, Department of Computer Systems University of Technology, Sydney, Australia, A review study on Digital Watermarking IEEE, 2005.

[16]. Vallabha V.H., Cranes Software International Limited Multiresolution watermark Based on Wavelet Transform for Digital images IEEE, 2002

[17]. Munesh Chandra, Shika Pandey, and Rama Chaudary, "Digital Watermarking Technique for Protecting Digital Images", IEEE 2010.

[18]. Jiang Xuehua "Digital Watermarking & its Application in image copyright Protection" published in proceedings of International Conference on Intelligent Computation Technology & Automation ICICTA2010.

