ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 4, July 2015

Copyright Protection of Multimedia files by Digital Watermarking

Manpreet Kaur & Jatinder Pal Sharma
Assistant Professor
Department Of CSE, GIMET, Amritsar
man.kaur39@gmail.com
profsharma88@gmail.com

Abstract

Watermarking is the process of embedding information or logo into a multimedia files (Audio, Video, Image), which may be used to verify the authenticity or identity of its owners. If someone modifies and misuses the file, then the logo/information embedded in it proves the authenticity. Various watermarking techniques have been proposed in literature. In this paper, we review the concept of watermarking which covers introduction, requirement, usage, attacks and various algorithms.

***Keywords:* Digital Watermarking, DCT, DWT, Spatial Watermarking.**

1. Introduction

With the continued rise of sharing over the Internet, it is getting increasingly more difficult to prevent copyright infringement of digital media. The increasing difficulty in protecting copyright ownership makes research in this field ever more important. There are many different types of digital watermarking, with different goals, and many schemes to accomplish those types of digital watermarking. In some watermarking schemes, a watermarked image has a logo or some other information embedded into the image so that it is readily visible; however these watermarks can be easily corrupted or removed using simple image processing techniques. Most watermarking schemes use invisible watermarking, in which the information is virtually invisible after it is embedded.

For digital data, copyright enforcement and content verification are very difficult tasks. One solution would be to restrict access to the data using some encryption techniques. However, encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated. Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object [1, 2].

Digital watermarking is described as one of the possibilities to close the gap between copyright issues and digital distribution of data. It acts as a very good medium for copyright issues as it embeds a symbol or a logo in the form of a watermark, which cannot be altered manually. One critical factor to be kept in mind when using watermarking is to prevent any further alterations to the originality of the image after embedding the data. Whenever the image with the secret data is transmitted over the internet unauthorized parties may want to hack the data hidden over the image. So, if the originality of the image has been changed then it will be easier to hack the information by unauthorized persons. In order to improve the security, the Digital watermarks are predominantly inserted as transformed digital signal into the source data using key based embedding algorithm and pseudo noise pattern. The digital watermarking technique essentially consists of a watermark inserter and a watermark detector as shown in figure 1.

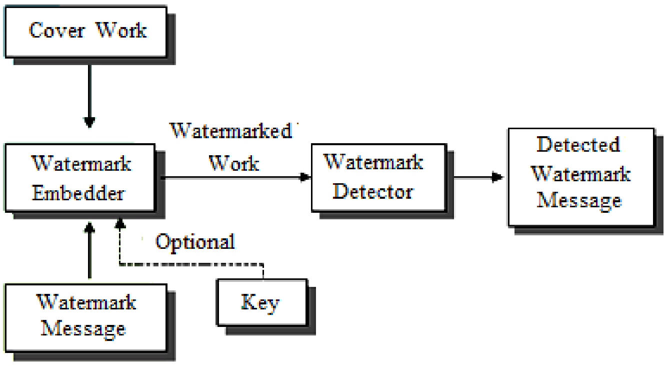

Fig. 1: Digital Image Watermarking

The watermark inserter inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo. Sometime a watermark key is also used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark information/. The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital image watermarking techniques should be resilient to both noise and security attacks .

II. Watermarking Classification

Various types of watermarking techniques having different applications are given below [3].

- ***Inserted Media Category:*** Watermarking techniques can be categorized on the basis of whether they are used for Text, Image, Audio or Video.
- ***Robust & Fragile Watermarking:*** In robust watermarking, the modification to the watermarked content will not affect the watermark whereas fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with.
- ***Visible & Transparent Watermarking:*** Visible watermarks are ones, which are embedded in visual content in such a way that they are visible when the content is viewed. Transparent watermarks are imperceptible and they cannot be detected by just viewing the digital content.
- ***Public & Private Watermarking:*** In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not authorized to detect the watermark.
- ***Asymmetric & Symmetric Watermarking:*** Asymmetric is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking the same keys are used for embedding and detecting watermarks.
- ***Steganographic & Non-Steganographic watermarking:*** Steganographic watermarking is the technique where content users are unaware of the presence of a watermark. In non-steganographic watermarking, the users are aware of the presence of a watermark. Steganographic watermarking is used in fingerprinting applications while non steganographic watermarking techniques can be used to deter piracy.

III. Watermarking Attacks

A robust watermark should survive a wide variety of attacks both incidental (Means modifications applied with a purpose other than to destroy the watermark) and malicious (attacks designed specifically to remove or weaken the watermark) [4]. We categorize the attacks as:

- ***Simple attacks:*** Simple or waveform or noise attacks are conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark.

Examples include filtering, compression (JPEG, MPEG), and addition of noise, addition of an offset, cropping, Digital to analog and analog to digital conversion.

- ***Detection-disabling attacks****:* Detection-disabling or synchronization attacks are attacks that attempt to break the correlation and to make the recovery of the watermark impossible or infeasible for a watermark detector, mostly by geometric distortion like zooming, shift in (for video) direction, rotation, cropping, pixel permutations, sub-sampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data.
- ***Ambiguity attacks****:* Ambiguity or deadlock attacks are attacks that attempt to confuse by producing fake original data or fake watermarked data. An example is an inversion attack that attempts to discredit the authority of the watermark by embedding one or several additional watermarks such that it is unclear which the first, authoritative watermark was.
- ***Removal attacks****:* Removal attacks are attacks that attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark. Examples are collusion attacks, denoising, certain filter operations, or compression attacks using synthetic modelling of the image.

IV. Watermarking Applications

Digital watermarking can also be in other applications not dealing with copy or copyright protection [5]:

- ***Indexing****:* Indexing of video mail, where comments can be embedded in the video content: indexing of movies and news items where markers and comments can be inserted that can be used by search engines.
- ***Medical application****:* Embedding the date and the patient's name in the medical images could be useful safety measure.
- ***Data embedding****:* Watermarking techniques can be used to embed messages in the data. The data can be secret or private, but it can also be public. .
- ***Error detection /Tamper proofing***: many researchers present an error detection scheme in video coding using a fragile watermark. This proposed scheme performs significantly better than a syntax-based error detection scheme.
- ***Compression****:* The researchers use watermarking techniques to improve the compression rate of color images. In this scheme, the colour information of the image is embedded as a watermark into the luminance data to reduce the data storage requirements.

V. Watermarking Algorithms

Most watermarking research and publications are focused on images. The reason might be that there is a large demand for image watermarking products due to the fact that there are so many images available at no cost on the World Wide Web, which need to be protected. Image watermarking techniques is broadly classified into spatial domain and transform domain techniques [6].

***A. Spatial Domain Approaches**:* Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during watermark embedding.
- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal.

The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. However, they also exhibit a major drawback: The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks.

Here, the secret messages are embedded directly. On spatial domain, the most common and simplest watermarking method is the least significant bits (LSB) insertion method. It is easy to be attacked. It reserves the image quality, increases embedding capacity but is not robust against attack because it is a spatial domain approach and no transfer is used. Based on the same embedding capacity, the proposed method improves both image quality and security[7]. In Computer-Based Watermarking, several forms of digital media may be used as “cover” for hidden information. Photos, documents, web pages, and even MP3 music files may all serve as innocuous-looking hosts for secret messages. In covert communications through the Internet, digital images are possibly the most practical type of Watermarking medium primarily due to their sheer abundance in the Web. However, one common problem with using digital images is use of insufficient hiding capacities. Most watermarking software hide information by replacing only least-significant bits of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding.

➢ *Least Significant Bit Insertion*

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking:

Image Pixel (binary):
10010101 00111011 11001101 01010101…
Watermark bits:
1 0 1 0…..
Watermarked Image:
1001010**1** 0011101**0** 1100110**1** 0101010**0**…..

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade. The spatial domain watermarking is simple as compared to the transform domain watermarking. The robustness is the main limitation of the spatial domain watermarking.

B. Transform Domain Approaches:

The transform domain watermarking is achieving very much success as compared to the spatial domain watermarking. In the transform domain watermarking, the image is represented in the form of frequency. In the transform domain watermarking techniques, firstly the original image is converted by a predefined transformation. Then the watermark is embedded in the transform image or in the transformation coefficients [8]. Finally, the inverse transform is performed to obtain the watermarked image. Most commonly used transform domain methods is Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT).

➢ *Discrete Cosine Transform (DCT)*

The main steps which used in DCT:

- Segment the image into non-overlapping blocks of 8x8.
- Apply forward DCT to each of these blocks.
- Apply some block selection criteria (e.g. HVS).
- Apply coefficient selection criteria (e.g. highest).
- Embedded watermark by modifying the selected Co-efficient.

- Apply inverse DCT transform on each block.

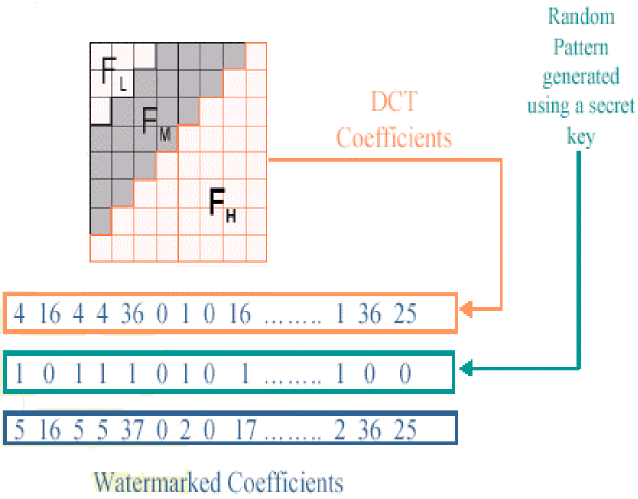

Fig. 2: DCT Domain Watermark

For an image Huffman coding assigns binary code to each intensity value of the image and 2-D $M_2 \times N_2$ image is converted to a 1-D bits stream with length $L_H < M_2 \times N_2$. The Huffman table (HT) contains binary codes to each intensity value. Huffman table must be same in both encoder and the decoder. Thus the Huffman table must be sent to decoder along with compressed image data. The Huffman code H is decomposed into 8-bits blocks B. Let the length of Huffman encoded bits stream be LH. Thus if LH is not divisible by 8, then last block contains r = LH% 8 number of bits (% is modulo operator).

➢ *Discrete Wavelet Transform (DWT)*

The basic idea is to decompose the original image into a series of details at different scales by using Wavelet Packets; a binary image used as a watermark is then embedded into the different levels of details. The embedding process includes: usage of an unique (secret) binary identification key to select the Wavelet decomposition scheme, Wavelet Packet decomposition, selection of the Wavelet coefficient groups to be used for hiding the watermark, insertion of the watermark in the corresponding group of coefficients by modifying the mean value of the group and Inverse Wavelet Transform. This algorithm does minimal degradation to the original image and can improve the robustness of watermarking against different attacks.

The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple “scale” wavelet decomposition, as in the 2 scale wavelet transform shown below in figure 3.

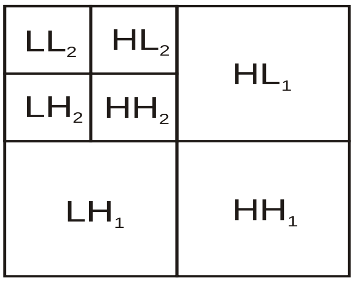

Fig. 3: 2 Scale 2-D Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [9, 10]. This algorithm uses a 128-bit key. The main steps of the algorithm are

- First the owner's identification key of 128 bits is randomly generated. 128 bits are enough to grant uniqueness of the key and protect the owner. This key is stored and kept secret.
- The first 8 bits in the secret key are used to select the wavelet decomposition scheme (the Wavelet functions used and the number of decomposition levels). The Wavelet families used are Coiflets, Daubechies and bi-orthognal and maximum decomposition level is L.
- Using the specification extracted from the secret key the Wavelet Packets decomposition of the original image is performed. The multidimensional decomposition is done using successive filter banks.
- The next 16 bits of the secret author's key indicate the size of the binary image used as the mark. The other bits of the key are used to identify the groups of coefficients, where the mark will be embedded. For every bit of the mark a group of N Wavelet Packet coefficients is identified. These groups of coefficients are evenly distributed in the bands of decomposition levels between 2 and L-1, where L is the maximum decomposition level of the original image.
- For every group of coefficients the mean is individually computed. Then the individual quantization levels q(i, j) are obtained The quantization step is chosen so as to maximize the embedding weight, while minimizing the distortion introduced. Afterwards, each bit of

the binary watermark image is inserted in the corresponding group of coefficients by the modification of the individual mean of the group. Rounding the mean to an even quantization level embeds a zero, while rounding the mean to an odd quantization level embeds a one. This is done by rounding the obtained quantization levels q(i, j) to the nearest even / odd quantization levels and then adjusting the mean of the wavelet packets coefficient regions to the computed values.

VI. Conclusions

This paper discusses the concept of watermarking for copy right protection of files. The requirement, classification, attacks and algorithms of image watermarking was briefly discussed in this paper. LSB substitution is the simplest technique but not a very good candidate for digital watermarking due to its lack of robustness. LSB embedded watermarks can easily be removed or altered without degrade the image quality. It would appear that LSB will remain in watermarking due to its tremendous information capacity. Most of the distortion-based watermarking techniques mainly aim at protecting the ownership, whereas distortion-free watermarking techniques mostly are fragile and aim at maintaining integrity.

References

1. E. Vellasques, E. Granger, R. Sabourin, Intelligent watermarking systems: a survey, 4th ed., Handbook of Pattern Recognition and Computer Vision, World Scientific Review, 2010, pp. 687–724.
2. Chen Lu, Geng Zexun, Chai Wenfu.Based on linear regression model Constraints spatial digital watermarking.Computer Engineering and Design, 2011, 32(2): 603-606 .
3. Run R, Horng S, Lin W, Kao T, Fan P, Khan MK. An efficient waveletetreeebased watermarking method. Expert Systems with Applications 2011;38(12):14357e66.
4. E. Vellasques, E. Granger, R. Sabourin, “Intelligent watermarking systems:” a survey, 4th ed., Handbook of Pattern Recognition and Computer Vision, World Scientific Review, 2010, pp. 687–724.
5. Bhatnagar Gaurav, Raman Balasubramanian. A new robust reference logo watermarking scheme. Multimedia Tools and Applications 2011;52(2):621e40.
6. Baisa L. Gunjal , R.R. Manthalkar “An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms”, Journal of Emerging Trends in Computing and Information Sciences, 2010-11.

7. Chih-Chin Lai, C.-C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition, IEEE Transactions on Instrumentation and Measurement 59 (11) (2010).
8. Cl. Song, S. Sudirman, M. Merabti, Recent advances and classification of watermark techniques in digital images, in: Proceedings of the 10th of PostGraduate Network Symposium, 2009, pp. 283–288.
9. Tsai, P., Hu, Y.C., Yeh, H.L., 2009. Reversible image hiding scheme using predictive coding and histogram shifting. Signal Processing 89 (6), 1129–1143.
10. Chen Lu, Geng Zexun, Chai Wenfu.Based on linear regression model Constraints spatial digital watermarking.Computer Engineering and Design, 2011, 32(2): 603-606 .