ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

A Review Paper on Digital Watermarking Techniques

[1] Sibaram Khara
[1] Department Of Electronics and Communication Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] sibaram.khara@Galgotiasuniversity.edu.in

Abstract: Image watermarking is gaining more popularity due to the wide use of internet and multimedia applications. Image watermarking adds some more information about host image in the form of audio or video or text. Main aim of watermarking is to provide copyright protection, Content authentication, Ownership identification, data integrity. Watermarking does not only protect content from modification only but also provide data integrity and content authentication. Main requirements of watermarking are robustness, security, capacity that varies according to different application. Copyright protection of plain text over the internet is very crucial task. Digital watermarking provides the complete copyright protection solution for this problem. Text being the most dominant medium travelling over the internet needs a lot of protection. Text watermarking techniques have been developed in past to protect the text from illegal copying, redistribution and to prevent copyright violations. This paper presents a review on some of the recent techniques used in watermarking for plain text documents. This is one of the most effective ways to safeguards the digital properties of our object.

Keywords: Content protection,DCT, DFT, DWT, Watermarking, Digital techniques, Transforms, Audio.

INTRODUCTION

With the rapid development of multimedia applications and internet technologies, protection of copyrights and security of content became an imperative concern. Authenticity of content is very important for solving the problem of copying, modification and distortions [1]. Different techniques are used for data hiding such ascryptography. It is different from digital signature and encryption.Digital signature is encrypted signed value or hash value. It can detect that image modification has been done but cannot track the location of modification. Likewise encryption allows users to use and access the data but does not provide the ownership identification. So as an efficient technique,digital watermarking is used to provide copyright protection and ownership identification.Watermarking technique is used for information hiding which is used to conceal proprietary information in digital media as photographs, digital video, digital music etc.The ease with which digital content can be exchanged over the Internet has created copyright infringement issues [2]. Over peerto-peer networks, copyrighted material can be easily exchanged and this makes serious concerns to those content providers who produce digital contents. This paper provides a survey of watermark techniques for files like video, text, images and audio.

Fig. 1: Visible and Invisible Watermarked Image

REVIEW ON DIGITAL WATERMARKING

Digital Watermarking techniquemeans the process to embed the given watermark informationsuch as symbol, possessory name, signature etc. into the protective informationsuch as sound, picture, videoand picking the given watermark information from the protective information, which is not perceived by human perceptual system.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

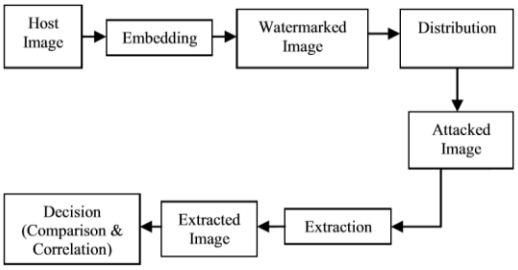

Fig.2: Process of Digital Watermarking

THREE STAGES IN WATERMARKING

1. Generation and Embedding

Pseudo random series, M- sequence and chaotic sequence are some sequences used for watermark generation [3]. The combination of watermark signal and copying of records, selected areas in original image Communications can be interpreted as embedding operation.

2. Distribution and Possible Attacks

The cycle of propagation can be understood as the signal being transmitted through the watermark tube. Possible attacks may be accidental or intentional on the broadcast channel.

3. Detection

Detection process allows the owner to be identified and provides information to the intended recipient.

CHARACTERISTICS OF DIGITAL WATERMARKING

Robustness:The watermark should be able to withstand after normal signal processing operations such as image cropping, transformation, compression etc.

Imperceptibility: The watermarked image should look like same as the original image to the normal eye. The viewer cannot detect that watermark is embedded in it.

Security: An unauthorized person cannot identify, extract or alter the watermark embedded therein. Robust watermarks can be identified even after some processing operations on the watermarked image, such as image scaling, bending and cropping, etc. Robust watermarks are used primarily to protect copyrights. Fragile watermarks became invalid even if the watermarked image underwent a slight modification. Fragile watermarks are used mostly for authentication. Semi-fragile watermarks cause the watermarked image to be distorted acceptably.

TEXT WATERMARKING TECHNIQUES

Spread Spectrum Technique of Watermarking:

This is mixing of watermarked bitswith the signal generated by Pseudo Random Noise and inserting this signal into the host signal [4]. This PRN signal operates as a secret key.

Line-Shift Coding:

Here each line is shifted slightly downwards or according to the payload bit value. If the bit is one, the corresponding line is shifted up; otherwise the line is shifted downwards. The odd lines are used in encoding and serve as control lines.Here each line is shifted slightly downwards or according to the payload bit value. If the bit is one, the corresponding line is shifted up; otherwise the line is shifted downwards. The odd lines are used in encoding and serve as control lines.

Word-Shift Coding:

Here we break down each line into a group of words. Every group contains a necessary number of characters. Then, each community is shifted to the right or the left according to the bit value in the payload. The different groups are used as comparisons to quantify and compare the differences at decoding between the groups.

Feature Coding:

Here certain text features for example; vertical end linesare changed in a specific way to encode the ones and zeros of the payloads. To detect Watermark the original document is compared with the watermarked document [5].

IMAGE WATERMARKING TECHNIQUES

Images can be represented as pixels in terms of frequencies in transform domain or spatial domain. We use reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Discrete Fourier Transform (DFT) to transfer an image to its frequency representation [6]. Watermarks can be embedded within images by

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

changing these values, i.e. the transform domain coefficients or pixel values.

DCT Domain Watermarking:

The high frequency components are watermarked in frequency domain. The main steps are:

(1) Divide the image into non-overlapping blocks of 8x8.

(2) Apply forward DCT to each of these blocks

(3) Apply some block selection criteria

(4) Apply coefficient selection criteria

(5) Embed watermark by modifying the selected coefficients.

(6) Apply inverse DCT transform on each block.

DWT Domain Watermarking:

Here the underlying concept is the same as DCT however; the process to transform the image into its transform domain changes and in this way the resulting coefficients comes different. Wavelet transforms use wavelet filters such as Daubechies Orthogonal Filters, HaarWavelet Filter and Daubechies Bi-Orthogonal Filters to transform the image. Each of these filters breaks the image into many frequencies. Single level decomposition yields four frequency representations of an image like LL, HH, LL, HH sub bands.

DFT Domain Watermarking:

DFT domain is favored as it offers robustness against geometric attacks such as translation, rotation, cropping, scaling, etc. There are two types of embedding techniques based on DFT watermark. In the first technique, watermark is embedded directly and the embedding based on templates is another technique. Embedded in direct embedding watermark is a structure that is used in the DFT domain to judge the transformation factor by changing the phase information within the DFT.A template. First a transformation is performed in image, then tore synchronize the image searched for this example, and then use the detector to extract the watermark of the embedded spread spectrum [7].

AUDIO WATERMARKING TECHNIQUES

The portion of data that can be embedded in audio is considerably smaller than the sum that can be embedded in images as the audio signal has dimensions of image files that are less than two dimensional. Due to the dynamic dominance of HVS than HAS, hiding additional information in the audio sequence is more complicated than images.

Least Significant Bit Coding:

This simple approach in watermarking audio sequences is to embed watermark data bychanging certain LSBs of the digital audio stream with low amplitude [8].

Phase coding:

The basic idea is to divide the original audio stream into blocks and then insert the whole watermark data sequence into the phase spectrum of the first block.

Spread-Spectrum Method:

This scheme spreads pseudo-random sequence across the audio signal. The wideband noise can be spread into either transformdomain signal or time-domain signal. Frequently used transforms include DWT, DFT, and DCT.

Replica Method:

It is possible to use the original signal as an audio watermark. Hiding echo is a pretty good example. Even replica modulation embeds part of the original signal as a watermark in the frequency domain.

VIDEO WATERMARKING TECHNIQUES

Embedding in the spatial domain:

Spatial Domain[9] technique uses the statistical properties of the pixels in the host image to be inserted and of the watermark image. To add the watermark it uses redundant bits in the cover image. If the watermark is an image then any algorithm must replace the pixels in the cover image with the pixels in the watermark image. This technique is less complicated and highly capable. The Least Important Bit Transformation approach is one of the widely used approaches of spatial domain techniques. This approach is easy to implement and is very simple. The watermark pixel bits are located in the least significant fraction of the cover image pixels.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

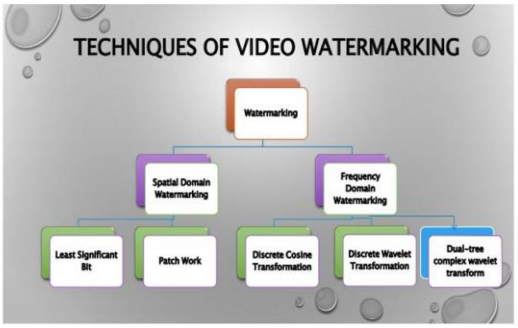

Fig.3:Video Watermarking Technique

Embedding in the transformation domain:

The technique of transforming domain uses numerous algorithms and transformations on the image to embed the watermark into it [10]. This technique masks information that isn't exposed to cropping and compression in those areas of the image. This uses the coefficients of the transform domain to store the message bits rather than to alter the pixel values. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are some commonly used transform domain techniques. Such methods take effect on the fact that they are less sensitive to high frequency coefficients of the Human Visual System (HVS).

CONCLUSION

The purpose of this paper is to describe the basicthe techniques of watermarking.Digital watermarking is said to be one of the best solutions for copyright protection over the World Wide Web, but some problems related to security of watermarking procedures to the various attacks needs to be addressed. This knowledge may be helpful in addressing the important questions that will be raised about watermarking, especially regarding the admissibility of watermarked data in courtrooms and the possible future standardization of one or more of watermarking algorithms. Nonetheless, for digital watermarking, the future seems bright. A lot of companies have already been involved in research into digital watermarking. For example, by embedding a watermark that remains permanently attached to audio files, Microsoft has created a prototype system that prevents unauthorized music playback. Such technology could be included in future versions of the Windows operating system as a default playback mechanism. If the music industry begins to include watermarks in its album archives, Windows will refuse to play copyrighted music that was released after a given date that was illegally obtained.

REFERENCES

[1] D. W. Lehman, K. O'Connor, B. Kovács, and G. E. Newman, "Authenticity," *Acad. Manag. Ann.*, 2019, doi: 10.5465/annals.2017.0047.

[2] R. Warkar, P. More, and D. Waghole, "Digital audio watermarking and image watermarking for information security," in *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, 2015, doi: 10.1109/PERVASIVE.2015.7086980.

[3] X. Ai *et al.*, "Pseudo-Random Single Photon Counting for space-borne atmospheric sensing applications," in *IEEE Aerospace Conference Proceedings*, 2014, doi: 10.1109/AERO.2014.6836513.

[4] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*. 2011.

[5] H. Adesnik, "Synaptic Mechanisms of Feature Coding in the Visual Cortex of Awake Mice," *Neuron*, 2017, doi: 10.1016/j.neuron.2017.08.014.

[6] R. G. Campos, "XFT: A Discrete Fourier Transform," in *Applied and Numerical Harmonic Analysis*, 2019.

[7] O. Christensen, "The fourier transform," in *Applied and Numerical Harmonic Analysis*, 2010.

[8] G. Kaur and K. Kaur, "Image Watermarking Using LSB (Least Significant Bit)," *Int. J.*, 2013.

[9] J. Russ and F. Neal, "Image Enhancement in

the Spatial Domain," in *The Image Processing Handbook, Seventh Edition*, 2015.

[10] P. Parashar and R. K. Singh, "A Survey: Digital Image Watermarking Techniques," *Int. J. Signal Process. Image Process. Pattern Recognit.*, 2014, doi: 10.14257/ijsip.2014.7.6.10.

[11] Vishal Assija, Anupam Baliyan and Vishal Jain, "Effective & Efficient Digital Advertisement Algorithms", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under ICT Based Innovations, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6602-3 from page no. 83 to 91.

[12] Vishal Jain and Dr. S. V. A. V. Prasad, "Analysis of RDBMS and Semantic Web Search in University System", International Journal of Engineering Sciences & Emerging Technologies (IJESET), Volume 7, Issue 2, October 2014, page no. 604-621 having ISSN No. 2231-6604.

[13] Vishal Jain and Dr. S. V. A. V. Prasad, "Evaluation and Validation of Ontology Using Protégé Tool", International Journal of Research in Engineering & Technology, Vol. 4, No. 5, May, 2016, page no. 1-12 having ISSN No. 2321-8843.

[14] RP Shermy, S Balamurugan, "Certain Investigation on Context Aware Knowledge Discovery Strategies for Healthcare Systems", Asian Journal of Research in Social Sciences and Humanities, Volume : 6, Issue : 8, 2016

[15] S Balamurugan, RP Shermy, Gokul Kruba Shanker, VS Kumar, VM Prabhakaran, "An Object Oriented Perspective of Context–Aware Monitoring Strategies for Cloud based Healthcare Systems",Asian Journal of Research in Social Sciences and Humanities, Volume : 6, Issue : 8, 2016

[14] S Balamurugan, P Anushree, S Adhiyaman, Gokul Kruba Shanker, VS Kumar, "RAIN Computing: Reliable and Adaptable Iot Network (RAIN) Computing", Asian Journal of Research in Social Sciences and Humanities, Volume : 6, Issue : 8, 2016