International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.8, No.10 (2015), pp.129-136
http://dx.doi.org/10.14257/ijsip.2015.8.10.15

A Review on Different Digital Watermarking Techniques

[1]Preeti Arya, [2]Dherendra Singh Tomar and [3]Deepika Dubey

Dept. of CSE, [1,2] MPCTGwalior, [3] SRCEM Banmore
[1] Pritiarya.arya217@gmail.com, [2] ds_er1@yahoo.com ,
[3]deepika.sa1304@gmail.com

Abstract

A digital watermark is a type of indicator covertly embedded in the noise tolerant signal such as an image or audio data. Digital watermarking is the method that embeds information known as a watermark into the multimedia object such that the watermark can be extracted or detected later to create an assertion about the object. Embedded watermark will permit recognizing the owner of the work hardware implementation. This idea is applicable for the digital video and audio also. Embedding a digital signal (image, video or video) with data which cannot be easily eliminated is called digital watermarking. Digital watermarks may be used to the authenticate the integrity or authenticity of the carrier signal or to display the identity of its owners Digital watermarking is used as a key result to create the document transferring protected from unlawful interferences. Digital watermark methods are used in numerous areas such as copyright owner identification, protection and broadcast monitoring. Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. In this paper, aim is to present a survey of numerous methods on the basis of digital image watermarking. The digital watermarking method is becoming more important in this developing society of internet. The goal of this implementation is to survey the different techniques for Digital Watermarking.

Keywords: *Digital watermarking, Embeds data, embedded watermark, DCT and DWT*

1. Introduction

It is the age of computers and network technologies. Progress in these has increases to massive scopes for developing and distribution of digital media theme. Digital data, are easy to be edited and irregular transcribe, thus we need a technology to obviate such issues [1].The spell "Digital watermarking" was first emerged in 1993.The Digital watermarking is a technology that organizes and assigns security, data certification, publishing protection to the digital media theme. Watermarking is the embedding of allude, watermarks into the digital media theme like as portrait, audio and film. Then later embedded data is searched and pointed out to exhibit an actual identity of digital media contents. Digital watermarking is used for various purposes such as proof of identity, copying deterrence, diastole monitoring, data hiding and certification[1].one of the greatest technological advancements to change people's lives in the past decade or so has been the Internet. The development of high speed computer networks and that of Internet, in particular, has explored means of new business, scientific, entertainment, and social opportunities in the form of electronic publishing and promotion, real-time information delivery, transaction processing, product ordering, digital repositories and libraries, web pages, web newspapers and magazines, network video and audio, personal communication, lots more[2]. Today, the Internet affects all industries as its potential continues to be recognized and explored [3]. The increase in demand has meant great attention has been paid to the evolution of net technology, including increased data

ISSN: 2005-4254 IJSIP

transfer speeds. One of the more notable side effects of this evolution has been the volume of data transfer between users, including the trading of pirate material, whether software, video or audio. With high transfer speeds and the ability to communicate with any other user connected to the Internet, piracy has become a serious problem[3]. The ease by which a digital data can be copied and dispersed has led to the require for effective copyright protection tools.

A variety of software products have been just presented in an attempt to address these rising concerns It should be possible to hide data (information) within digital audio, video and images files. The information is hidden in the sense that it is perceptually and satistically invisible. One way to protect the multimedia data beside illegal recording and retransmission is to implant a signal, known copyright label or digital signature or watermark that totally characterizes the somebody who applies it and, consequently, marks it as being his intellectual property [4]. Digital watermarking

stands for embedding a signature signal, called watermark into a digital cover, in order to verify ownership, check authenticity or integrity of the cover, and it may relate to audio, images, video or even text. Digital watermarking is a method of the embedding unobtrusive marks or labels into digital content. These implanted marks are classically invisible (imperceptible) that can later be extracted or detected .The idea of the digital watermarking is related with steganography.

Steganography is defined as covered writing. It has a long history of being associated with methods of secret communication. Therefore, digital watermarking is a method to hide a private or secret message to the protect a product's copyright or to demonstrate data integrity. The watermark may hold a safety feature such as data serial no. or other knowledge related to the document to originator such as DOB. Watermarked data can give the knowledge about alterations or upgrading, counterfeits by comparing the watermarked data to original data [5]. The watermark content depends upon the originator or requirements to the confirm the integrity of the knowledge as well as authentication of the data.

2. Private and Pubic Watermaeking

Digital watermarking methods can be classified as public and private watermarks [5].

A. Private Watermark

A secret (private) watermark may hold knowledge for recognizing the prove ownership in disputes or licensee. Retrieval of private watermark data requires at least one private key, known only to the Embedder. A secret watermark puts heavy demands on a watermarking procedure regarding robustness, although the demands for ability are relaxed.

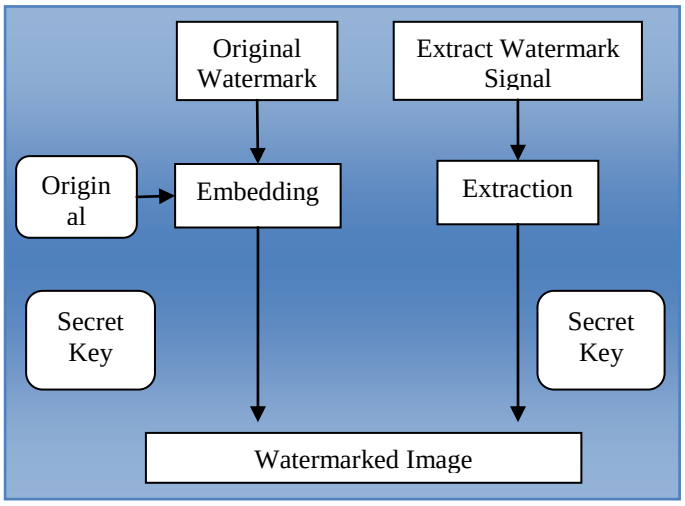
Embedded knowledge, commonly includes licensee-identifying hash values or sequential no. In common, a sequential no. is just a link or pointer to externally stored knowledge, such as a consumer record [6].

B. Public Watermark

A public watermark is retrieved by the licensee receiver (receiver) of copyrighted material. It usually holds licensing or copyright information, such as the identifier of the patent or copyright container, the designer of the material, or a link (Universal Resource Locator) through which to fetch more related information. A public watermark puts dense demands on a watermarking procedure regarding capacity. Because of a public watermark provides at an additional copyright related information for receivers and doesn't goal to verify ownership or ownership, the requirements regarding robustness are relaxed [7].

3. Digital Watermarking

The method of the watermark embedding in a multimedia object is termed as a watermarking. The watermark can be considered as a type of a signature that reveals the holder of the multimedia object. Content providers want to embed watermarks in the their digital content (multimedia objects) for various causes like tamper detection, copyright protection, content authentication, etc. A watermarking procedure embeds invisible or a visible watermark in a given multimedia object. The embedding method is guided by the use of a private key which defines the locations within the multimedia image (object) where as the embedded watermark. Once the embedded watermark is can knowledge numerous attacks because of the multimedia object can be processed digitally. The attacks can be intentional (like cropping) or unintentional (in case of images, gamma correction or low pass filtering or compression). Hence the watermark has to be more robust against every these probable attack. When the holder wants to check the watermarks in the distorted multimedia object and possibly attacked, s/he relies on the private key that was used for the embed watermark. Applying the private(secret) key, the embedded watermark series may be mined. This mined watermark may or may not resemble the old watermark because of the object might have been attacked. Hence, to authenticate the presence of watermark, either the previous object is used to find out and compare the non-blind watermarking (watermark signal) or a correlation measure is used to the identify the strength of the watermark signal from the blind watermarking (extracted watermark). In the correlation based finding the original watermark series is compared with the extracted watermark series and the statistical correlation test is used to define the existence of the watermark.



4. Watermarking Technique

The various watermarking techniques are:

A. Spatial Domain Techniques

Spatial domain watermarking slightly pixels changes one or two randomly chose subsets of an image. Alterations might contain flipping the low-order bit of every pixel. However, this method is not reliable when subjected to usual media operations such as lossy compression or filtering.
Various spatial domain techniques are as follows:-

Least Significant Bit Coding (LSB)

LSB coding is one of the earliest methods. It can be applied to any form of the watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back, this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique, but the robustness of the watermark will be too low. With LSB is coding almost always the watermark cannot be retrieved without a noise component.

Predictive Coding Schemes

A predictive coding scheme was proposed by Matsui and Tanaka in [8] for gray scale images. In this method the correlation between adjacent pixels are exploited. Pixels collection where the watermark has to the embedded is alternate and selected pixels are swapped by the difference between adjacent pixels. This can be additional improved by adding a constant to each of the differences. A cipher key is produced which allows the retrieval of the embedded watermark at receiver. This is much more robust as compared to LSB coding.

Correlation-Based Techniques

In this method a PN (pseudo random noise) with a pattern W (x, y) is added to an image. At the decoder the correlation between the image is found out and random noise and if the value exceeds a certain threshold value the watermark is detected else it is not.

Patchwork Techniques

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to the these two subsets in the opposed direction. For instance, if one subset is increased by a factor k, the other subset will be decreased by the same amount. If a [i] is the value of the sample at I in subset 'A' which is improved and b [i] is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in $\Sigma(a[i]-b[i]) = 2N$ for watermarked images $1<=N<=\infty = 0$ otherwise

B. Frequency Domain Techniques

In the Frequency domain private document is secreted in the middle or lower frequency portions of the secure image, because of the advanced frequency portion is the more likely to be suppressed by the compression. But how to the select the greatest frequency portions of any image for watermark is another difficult and important topic. Numerous frequency domain methods are as follows:-

Discrete cosine transform (DCT) based technique

DCT (Discrete cosine transform): It is a method which changes a series of document points in spatial domain to a addition of the cosine and sine waveforms with numerous amplitudes in the frequency domain. The DCT is a linear transform, which maps a n-dimensional vector to a set of n coefficients. It is very robust to JPEG compression, since JPEG compression it uses DCT. However, DCT methods lack resistance to strong geometric distortions.

Discrete Fourier Transformation (DFT) based technique

It is a translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.DFT uses complex numbers, while DCT uses just real numbers.

Discrete wavelet transform (DWT) based technique

DWT-based methods enable good spatial localization and have multi resolution characteristics, which are alike in the visual system of the human. Also, this method displays robustness to median and low-pass filtering. However, it is not robust to geometric transformations.

C. Wavelet Transform based Watermarking

The wavelet transform based watermarking technique divides the image into four sidebands – a low resolution approximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform

5. Requirements of the Digital Watermarking

Here three central requirements of the digital watermarking. They are capacity, robustness, and robustness.

A. Fidelity or F Transparency

The digital watermark should not disturb the quality of the old image after it is watermarked. Cox et al. (2002) describe fidelity or transparency as "perceptual similarity between the old and the watermarked versions of cover work". Watermarking should not present visible distortions, because if such distortions are present it decreases the commercial value of the image.

B. Robustness

Cox et al. (2002) describes robustness as the "ability to the detect watermark after general signal processing operations". Watermarks could be eliminated unintentionally or intentionally by simple image processing operations like brightness enhancement or contrast, gamma correction etc. Hence watermarks should be robust against variability of the such attacks. Stirmark2 categorizes attacks into four simple classifications, attacks that try to eliminate watermarks completely, attacks that try to eliminate the synchronization between the embedded and the detector, protocol attacks and cryptographic attacks.

Capacity or Data Payload

Cox et al. (2002) describe data or capacity payload as "the no. of bits a watermark encodes within a work or a unit of time". This property defines how much document should be embedded as a watermark to effectively detect at the time of extraction. The watermark should be able to carry enough knowledge to represent the uniqueness of the image. Several applications have different payload requirements [9].

6. Watermarking Application

Here we are discussing about main application of digital watermarking

C. Copyright Protection

Watermarking can be used to protect redistribution of copyrighted material over untrusted network like the Internet or P2P (peer-to-peer) networks. Content aware networks (peer-to-peer) could incorporate watermarking method to filter out or report copyrighted material from such networks.

D. Content Archivin

Watermarking can be used to insert a serial number or digital object identifier to help archive digital contents like video, images or audio. It can also be used for categorizing and establishing digital contents. Generally, digital contents are recognized by their names of file; however, this is a very fragile method as names of file can be simply altered. decreases the possibility of the tampering and hence can be efficiently used in archiving systems.

E. Metadata Insertion

Metadata refers to the information that define knowledge. Images can be labeled with its content and can be applied in search engines. Audio files can be carry the lyrics or the singer name. Journalists could use the photographs of an event to the insert the story cover on the relevant news. Medical X-rays could collection patient histories.

F. Broadcast Monitoring

Broadcast Monitoring refers to the method of the cross-verifying whether the content that was supposed to be the broadcasted (on the Radio or TV) has actually been broadcasted or not broadcasted. Broadcasted is the basic purpose of Watermarking can also be used monitoring purpose. This has main application is commercial advertisement broadcasting, where the object who is advertising wants to the monitor whether their advertisement was really broadcasted at the right time and for the right duration.

G. Tamper Detection

Digital content can be discovered for tampering by the embedding fragile watermarks. If a fragile watermark is degraded or damaged, it showed the presence of the digital content and hence tampering cannot be trusted. Tamper detection is most important for a few applications that include extremely sensitive document like medical imagery or satellite imagery. Tamper detection is also valuable in a court of law where digital images could be used as a forensic tool to show whether the image is tampered or not.

H. Digital Fingerprinting

Digital Fingerprinting is a method used by the discover owner of the digital content. Thumbprints are unique to the owner of the digital content. Hence a single digital object can have several fingerprints because they belong to various users

7. Literature View

In 2000, Chen *et al.'s* [13] proposed an adaptive watermarking scheme. This scheme embeds a binary image as watermark in DCT approach. The watermarked image is imperceptible by the human visual system. It uses a feature based method to locate the watermark positions during embedding and extracting. The feature-based method uses the Sobel edge-detector to obtain the gradient magnitude and this result is proportional to the amount of watermark bits.

In 2009, Chen et al.[12] proposed a spatial domain watermarking technique based on the idea of incorporating block-wise dependency information in the watermarking procedure for thwarting VQ attack without compromising on localization capabilities of the scheme. The block-wise dependency relationship between the blocks of the image is established using fuzzy clustering criteria; a fuzzy C-means algorithm is used for this purpose. This method allows one piece of data to belong to two or more clusters unlike other traditional hard clustering schemes like k-means algorithm that assigns data points to a specific cluster. The scheme consists of authentication data embedding procedure and tamper detection procedure.

In 2012, Kannammal et Al. [10] Proposed a digital watermarking framework in which the ECG (Electrocardiograph) and Patients demographic text identification act a0s the double watermarks. By this type of method the medical data about the patient is secure and mismatching of the diagnostic data is prevented. Transform domain techniques are in greater use nowadays in place of spatial domain techniques as much is known about the properties of these transforms to achieve better watermark characteristics.

In 2012, Chitla Arathi [11] obtainable a semi-fragile watermarking method which is based on block based SVD (singular value decomposition). Semi-fragile watermark is fragile to malicious modifications while robust to incidental manipulations.The scheme can be mine the watermark without the original image. SVD transformation preserves both one way and non-symmetric properties that are not obtainable in DCT and DFT transformations. This technique can also detect tamper made on the image.

In 2011, Bhattacharya et. Al.[14] proposed a novel approach which creates use of both robust and fragile watermarking methods. The embedded fragile watermark is used to the assess degradation undergone by the images transmitted. Robust image features are used to purpose of the construct the reference watermark from the received image, for assessing the amount of degradation of the fragile watermark.

In 2011, Yan et. Al. [15] presented a blind watermarking approach to protect vector Geo-spatial data from illegal use. The presented method is rarely affected by the data format change, random noise, similarity transformation of the data, and data editing.

In 2012, Chen et. Al. [16] suggested a watermarking method based on frequency domain. An adapted algorithm is presented to increase the defect of the JPEG quantification in order to reduce the BER (bit error rate) of the retrieved watermark. In Addition, two parameters called controlling factors are used to adjust the value of the DCT coefficient in order to trade-off the qualities between watermarked images and retrieve watermark. Moreover, the proposed procedure is designed as a blind mechanism. Thus, the original image and watermark are not needed for the removing watermark.

8. Conclusion

Digital watermarking is very useful method for providing security to the digital media on the internet technology Digital watermarking is still a challenging research field with many interesting problems, like it does not prevent copying or distribution and also cannot survive in every possible attack. In this paper, we surveyed the on digital image watermarking current literature. And also survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, DFT). We have obtainable various aspects of digital watermarking like introduction, outline, techniques, and applications.

References

[1] C.-I. Woo and S.-D. Lee, "Digital Watermarking for Image Tamper Detection using Block-Wise Technique", International Journal of Smart Home, vol. 7, no. 5, (**2013**), pp. 115-124 http://dx.doi.org/10.14257/ijsh.2013.7.5.12.

[2] P. Singh and R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology, (IJEIT), vol. 2, no. 9, (**2013**), March.

[3] M. I. Khan1, Md. M. Rahman and Md. I. H. Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation", IJCSI International Journal of Computer Science Issues, vol. 10, no. 3, no. 1, ISSN (Online): 1694-078, (**2013**) May.
[4] D. Mistry, "Comparison of Digital Water Marking methods", (IJCSE) International Journal on Computer Science and Engineering, vol. 02, no. 09, (**2010**), ISSN 2905-2909.
[5] J. Jain and V. Rai, "Robust Multiple Image Watermarking Based on Spread Transform", vol. 2, ISBN 978-953-51-0619-7, (**2012**) May 16.
[6] M. Tonge#1, P. k. Malviya*2 and A. Gupta, "Implementation of Digital Watermarking Algorithm based on DWT and DCT", International Journal of Advanced Engineering and Global Technology, Vol-2, Issue-1, January 2014 ISSN No: 2309-4893, (**2014**) January.
[7] V. Kumar, R. Lautan, MHD Faisal, K. M. Pandey, "Dwt and Particle Swarm Optimization Based Digital Image Watermarking", International Journal of Engineering Research & Technology (IJERT),Vol. 2 Issue 9,ISSN: 2278-0181, (**2013**) September 9.
[8] T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", Information Sciences: an International Journal, vol. 179, (**2009**) September.
[9] Cox, Li, Miller, ML and Bloom, JA, "Digital Watermarking, Morgan Kaufmann Publishe"r, San Francisco, CA, USA, (**2002**).
[10] A. Kannammal, K. Pavithra, S. Subha Rani, "Double Watermarking of Dicom Medical Images using Wavelet Decomposition Technique", Proceedings of European Journal of Scientific Research, vol. 70, no. 1, (**2012**), pp. 46-55.
[11] C. Arathi, "A Semi Fragile Image Watermarking Technique Using Block Based SVD", Proceedings of International Journal of Computer Science and Information Technologies, vol. 3, no. 2, (**2012**), pp. 3644-3647.
[12] W.-C. Chen nad M.-S. Wang, "A Fuzzy c-Means Clustering based Fragile Watermarking Scheme for Image Authentication", Proceedings of Expert Systems with Applications, vol. 36, no. 2, Part 1, (**2009**), pp. 1300-1307.
[13] D.-Y. Chen, M. Ouhyoung, and J.-L. Wu, "A Shift- Resisting Public Watermark System for Protecting Image Processing Software", Proceedings of IEEE Transactions on Consumer Electronics, vol. 46, no. 3, (**2000**), pp. 404-414.
[14] A. Bhattacharya, S. Palit, N. Chatterjee, and G. Roy, "Blind assessment of image quality employing fragile watermarking", 7th International Sym. on Image and Signal Processing and Analysis (ISPA 2011) Dubrovnik, Croatia, (**2011**), pp. 431- 436.
[15] H. Yan, J. Li and H. Wen, "A key points-based blind watermarking approach for vector geo-spatial data", (**2011**).

