International Journal of Advanced Research in Engineering Technology & Sciences ISSN: 2394-2819
January-2016 Volume 3, Issue-1
Email: editor@ijarets.org www.ijarets.org

A Survey Work On Digital Watermarking

Rajesh Kumar Rai
Department of Computer Science & Engineering
Harcourt Butler Technological Institute
Kanpur

Nisha
Department of Information Technology
Regional Engineering College
Bijnor

Rati Shukla , Punit Kumar Chaubey
Department of Computer Science & Engineering
Motilal Nehru National Institute of Technology
Allahabad

ABSTRACT:
Digital Multimedia contents like text, image, audio and video are widely used and are very easy to transmit over the Internet, and hence the copyright protection has been receiving and increasing attention these days. Other than copyright protection Digital Watermarking is now used for Digital Marketing and promotional Services. A Static Promotional media is now can be made highly productive Dynamic Promotional medium by using Digital watermarking. This work incorporate the detail study watermarking definition, concept and the main contributions in this field such as categories of watermarking process that tell which watermarking method should be used. This work provides evidence that digital watermarking techniques are of growing interest and are of fast popularity.

KEYWORDS: Digital Watermarking Trap, PSNR, DCT, Filters, De-noising Spatial and frequency domain, Asynchronous Encryption.

I. INTRODUCTION:

In 1993, Tirkel introduced the term "Digital Watermarking" and presented two watermarking techniques to hide the watermark data in the images [1]. Digital watermarking is a technique which allows attaining the objective of protecting the intellectual property rights by adding patent notices or other verification messages to digital media. One of the applications of digital watermarking is image endorsement, which is used for authenticating the digital images. Its main objective is to provide a method to validate the image and assure the integrity of the image. Watermarking is used for Proof of rights/copyrights protection, Data Hiding, Copying Prevention, Broadcast Monitoring etc. Watermark embedding, watermark detection and extraction are basic modules of Watermarking. Digital watermarking technology has many applications in anti-counterfeit of the digital media, label of the user information, protection, certification, distribution etc. Information hiding is its important study area. Digital watermarks can be classified into two different groups: blind detection [2] (original data is not required) and non-blind detection (original data required) when extracting watermark. As the Digital media is widely used in the current scenario for transmission over the internet the space required to store the image is a major factor, so here the concept of Image compression comes which means to reduce the amount of data required to represent a digital image. Popularly used techniques for image compression are DCT [3] and DWT [4] which are frequency based techniques and have its' own advantages and disadvantage. Also we have seen that, as DWT gives better compression ratio without losing more information of image but it need more processing power. While in DCT need low processing power but it has blocks artefacts means loss of some information but has most important feature of Energy Concentration.

Motivated by the above discussion, the two-level DCT is introduced to further concentrate the energy and a novel blind watermarking method based on two-level DCT for dual colour image was proposed by QingtangSua,YugangNiub, XianxiLiuc and Tao Yaoa [5]. This paper analyses the key technologies of digital watermarking and explores the application in the digital image copyright protection. Other than copyright protection Digital Watermarking is now used for Digital Marketing and promotional Services. A Static Promotional media is now can be made highly productive Dynamic Promotional medium by using Digital watermarking. So for making it more secure [6], authentic and copyright a blind digital watermarking using AES technique [7] and Noise filters for colour images is proposed in this paper.

The organization of the paper is as follows: Section 2 describes Digital Watermarking. Basic requirements are shown in Section 3. In Section 4 various watermarking techniques are shown. In Section 5 we have Application of Digital watermarking and Section 6 concludes the paper.

II. DIGITAL WATERMARKING:

Digital watermarking hides the patent information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special significance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and patent protection [8].

The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in unlike scenario. If the signal was notmodified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. If the signal is copied, thenthe information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the framearound the data, it is carried with the signal itself. Figure 1 shows the basic block diagram of watermarking process. The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

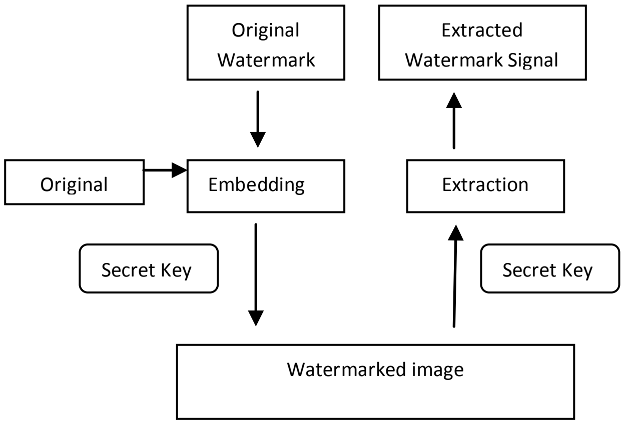

Figure 1. Block diagram of Watermarking Process.

III. BASIC REQUIRMENTS:

The major requirements for digital watermarking are [8]:

A. BASIC:

1) TRANSPARENCY:

The embedded watermark should not corrupt theoriginal image. If visible distortions are introduced in theimage, it creates disbelief and makes life no difficulty for theattacker. It also degrades the commercial value of the image.

2) ROBUSTNESS:

This is by far the most important requirement of awatermark. There are various attacks, unplanned(cropping, compression, scaling) and planned attackswhich are aimed at destroying the watermark. So, theembedded watermark should be such that it is invariant to various such attacks.

3) CAPACITY OR DATA LOAD:

This quantity describes the maximum amount of datathat can be embedded into the image to ensure properrecovery of the watermark during extraction.

B. ATTACHED MEDIA/HOST SIGNAL:

1) IMAGE WATERMARKING:

This is used to hide the special information into the image and to later detect and extract that special information for the author‘s rights.

2) VIDEO WATERMARKING:

This adds watermark in the video stream to manage video applications. It is the extension of image watermarking. This method requires real time extraction and strength for compression.

3) AUDIO WATERMARKING:

This application area is one of the most popular and hot issue due to internet music, MP3.

4) TEXT WATERMARKING:

This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

5) GRAPHIC WATERMARKING:

It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright [8].

C. PERCEPTIVITY:

1) VISIBLE WATERMARK:

The watermark that is visible in the digital data like stamping a watermark on work, (ex.) television channels, like HBO, whose logo is visibly superimposed on the spot of the TV picture.

2) INVISIBLE WATERMARKING:

There is technology available which can insert information into an image which cannot be seen, but can be interrogated with the right software. You can‘t prevent the theft of your images this way, but you can prove that the image that was stolen was yours, which is almost as good. Invisible watermark can be further divided into three types:

a) ROBUST WATERMARK:

It aims to embed informationin a file that cannot be easily destroyed. They are designedto resist any manipulations that may be encountered. Allapplications where security is the main issue use robustwatermarks.

b) FRAGILE WATERMARK:

They are designed with verylow robustness. They are used to check the integrity ofobjects.

c) PUBLIC AND PRIVATE WATERMARK:

They are differentiated in accordance with the secrecy requirementsfor the key used to embed and retrieve watermarks. If theoriginal image is not known during the detection processthen it is called a public or a blind watermark and if theoriginal image is known it is called a non blind watermark or a private watermark [8].

D. ACCORING TO WATERMARK TYPES:

1) NOISE TYPE:

Noise type has simulated noise, Gaussian accidental and disordered sequences.

2) IMAGE TYPE:

There are binary image, stamp, logo and label.

IV. VARIOUS WATERMARKING TECHNIQUES:

The various watermarking techniques are:

A. SPATIAL DOMAIN TECHNIQUES:

Spatial domain watermarking a little modifies the pixels of one or two accidentally selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not dependable whensubjected to normal media operations such as filtering or lossy compression. Various spatial domain techniques are as follows:-

1) LEAST SIGNIFICANT BIT CODING (LSB):

LSB coding is one of the earliest methods. It can beapplied to any form of watermarking. In this method theLSB 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 valueson which the watermark has to be embedded. It thenembeds the information on the LSBs of the pixels from thissubset LSB coding is a very simple technique but therobustness of the watermark will be too low. With LSBcoding almost always the watermark cannot be retrievedwithout a noise component [9].

2) PREDICTIVE CODING SCHEMES:

Predictive coding scheme was planned by Matsui and Tanaka in [2] for gray scale images. In this method thecorrelation between neighboring pixels are broken. A set ofpixels where the watermark has to be embedded is chosenand alternate pixels are replaced by the difference betweenthe adjacent pixels. This can be further enhanced by addinga constant to all the differences. A cipher key is createdwhich enables the retrieval of the embedded watermark atthe receiver. This is much more robust as compared to LSB coding.

3) CORRELATION-BASED TECHNIQUES:

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

4) PATCHWORK TECHNIQUES:

In patchwork watermarking, the image is divided intotwo subsets. One feature or an operation is chosen and it isapplied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the othersubset will be decreased by the same amount. If a[i] is the value of the sample at I in subset 'A' which is increased and b[i] is the value of the sample in the subset 'B' whose valueis decreased, then the difference between the two subsetswould intuitively result in -->

$\Sigma(a[i]-b[i]) = 2N$ for watermarked images $1<=N<=\infty= 0$ otherwise

B. FREQUENCY DOMAIN TECHNIQUES:

In Frequency domain the secret data are hidden in the lower or middle frequency portions of the protected image, because the higher frequency segment is more likely to be suppressed by compression. But how to select the best frequency portions of the image for watermark is another important and difficult topic. Various frequency domain techniques are as follows:-

1) DISCRETE COSINE TRANSFORM (DCT) BASED TECHNIQUE:

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to asum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. It is very robust to JPEG compression, since JPEG compression itself uses DCT. However, DCT methods lack resistance to strong geometric distortions.

2) DISCRETE FOURIER TRANSFORMATION (DFT) BASED TECHNIQUE:

It is translation invariant and rotation resistant, whichtranslates to strong robustness to geometric attacks.DFTuses complex numbers, while DCT uses just real numbers.

3) DISCRETE WAVELET TRANSFORM (DWT) BASED TECHNIQUE:

DWT-based methods enable good spatial localizationand have multi resolution characteristics, which are similarto the human visual system. Also this approach showsrobustness to low-pass and median filtering However, it is not robust to geometric transformations.

C. WAVELET TRANSFORM BASED WATERMARKING

The wavelet transform based watermarking techniquedivides the image into four side bands – a low resolutionapproximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics.The process can then be recurring iteratively to produce N scale transform [10].

Digital watermarking techniques are classified according to various criteria like robustness, perceptibility, embedding and retrieval methods. Robustness is an important criterion which means the ability of watermark to resist common image processing operations.

Watermarking techniques based on robustness can be further divided into three main categories:

(1) Robust (2) Fragile (3) Semi-fragile

Robust watermarking schemes are applied for proving possession claims whereas fragile watermarking is applied to multimedia content authentication. These watermarkingschemes have their own requirements in terms of robustness. Robust watermarks should be able to survive a wide range of friendly operations and malicious attacks, whereas weak watermarks are impossible to both horrible and content preserving operations.

Fragile watermarkingtechniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image verification. Some grave applications similar to medical imagining and forensic image archiving also require the fragile watermarks to be reversible. The differentquantitative parameters such as PSNR, True and false positive may be used for the estimate of the technique of watermarking schemes.

V. APPLICATIONS:

Digital watermarking can be used for the following purposes:

A. COPYRIGHT PROTECTION:

This is by far the most famous application of watermarks. With tons of images beingexchanged over lacking confidence networks every day, patent protection becomes a very important issue. Watermarking an image will prevent redistribution of pretended images.

B. B.AUTHENTICATION:

Sometimes the ownership of thecontents has to be verified. This can be done byembedding a watermark and providing the owner with aprivate key which gives him an admission to the message. IDcards, ATM cards, credit cards are all examples ofdocuments which require confirmation.

C. BROADCAST MONITORING:

As the name suggests broadcastmonitoring is used to verify the programs broadcasted onTV or radio. It especially helps the advertisingcompanies to see if their advertisements appeared for theright duration or not.

D. CONTENT LABELING:

Watermarks can be used to give moreinformation about the cover object. This process is named as content labeling.

E. TAMPER DETECTION:

Fragile watermarks can be used todetect tampering in an image. If the fragile watermark isdegraded in any way then they can say that the image ordocument in question has been tampered.

F. DIGITAL FINGERPRINTING:

This is a process used to detect the owner of the content. Every fingerprint will beunique to the owner.

G. CONTENT PROTECTION:

In this process the content printed with a visible watermark that is very hard to removeso that it can be openly and freely distributed.

VI. CONCLUSIONS:

This survey reveals the scope of the digital watermarking and also led us to know its importance and application. As we have mentioned that other than copyright protection Digital Watermarking is now used for Digital Marketing and promotional Services. A Static Promotional media is now can be made highly productive Dynamic Promotional medium by using Digital watermarking. So for making it more secure, authentic and copyright a Blind digital watermarking using AES technique for color images could be proposed for future work and hence for the security of digital watermark some more researches should be done.

With the introduction of Digital Marketing and Promotional Services using Digital watermarking the Future Scope for this scheme will be for providing more secure algorithm and approach so as to protect from the Hackers and market competitors.

REFERENCES:

1. R.G. Schyndel, A. Tirkel and C. F. Osborne, A Digital Watermark, Proceedings of IEEE International conference on Image Processing, pp. 86-90, (1994).
2. X.Y. Luo, D.S. Wang, P. Wang, F.L. Liu, A review on blind detection for image steganography, Signal Process. 88 (2008) 2138–2157.
3. Z. Yong, L.L. Cai, L.Q. Shen, J.Z. Tao, A blind watermarking algorithm based on block DCT for dual colour images, in: 2009 Second International Symposium on Electronic Commerce and Security, 2009, pp. 213–217.
4. Nirupma Tiwari, Manoj Kumar Ramaiya, Monika Sharma “Digital Watermarking using DWT and DES”2013 3rd IEEE International Advance Computing Conference (IACC).
5. QingtangSua, YugangNiub, XianxiLiuc and Tao Yaoa, A novel blind digital watermarking algorithm for embedding colour image into colour image, Optik Elsevier B., Vol. 124, pp.3254– 3259, (2012).
6. Metkar, S.P. ; Lichade, M.V., Digital image security improvement by integrating watermarking and encryption technique, Signal Processing, Computing and Control (ISPCC), 2013 IEEE International Conference, pp. 1-6.
7. Manoj Ramaiya, Naveen Hemrajani, Anil kishor Saxena “Secured Steganography approach by using AES” International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831Vol. 3, Issue 3, Aug 2013, 185-192.
8. Prabhishek Singh,R S Chadha, ― A Survey of Digital Watermarking Techniques, Applications and Attacks, nternational Journal of Engineering and Innovative Technology (IJEIT)Volume 2, Issue 9, March 2013.
9. Nidaa A. Abbas, “Image watermark detection techniques using quadtrees”, Applied Computing and Informatics, August 2014.
10. Pragya Jain, Anand S. Rajawat, “Fragile Watermarking for Image Authentication: Survey”, International Journal of Electronics and Computer Science Engineering,ISSN- 2277-1956.