Review to Digital Watermarking and a Novel Approach to Position the Watermark in the Digital Image

Prabhishek Singh, R S Chadha

Abstract— Digital watermarking technology is a frontier research field and it mainly focuses on the intellectual property rights, identification and authentication of the digital media to protect the important documents. According to the basic analysis of digital image watermarking the digital watermarking model consists of two modules, which are watermark embedding module and watermark extraction and detection module Since it is known that digital image transmitted and spread over the network so there is a chance of being polluted by the noise or it may be attacked by the malicious users. The watermark embedded in the digital image may be incorrectly detected due to shortage of algorithms, so to precisely position the watermark is the main issue. A review to Digital watermarking is being presented in the paper and a novel watermark positioning approach is proposed in this paper which uses the statistical characteristics of the pixels to embed the watermark into brightness values of the pixels using image segmentation on the Windows platform using Matlab programming language.

Keywords— Digital Watermarking, Image segmentation, Matlab functions, Otsu's method thresholding, Patchwork algorithm.

I. INTRODUCTION

We are living in the era of information where billions of bits of data is created in every fraction of a second and with the advent of internet, creation and delivery of digital data (images, video and audio files, digital repositories and libraries, web publishing) has grown many fold. Since copying a digital data is very easy and fast too so, issues like, protection of rights of the content and proving ownership, arises. Digital watermarking came as a technique and a tool to overcome shortcomings of current copyright laws for digital data. Watermarking is embedding a hidden message within the original data "host image". Watermarking is used for following reasons, Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication, Data Hiding. Digital Image Watermarking discourages the unauthorized copying and distribution of image over the internet. It ensures a digital picture has not been altered.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

Manuscript received April, 2013.

Prabhishek Singh, M.Tech (CSE), Department of CSE, C-DAC, Noida, India.

R S Chadha, Assistant.Prof, MTech Head, CDAC, Noida, India.

In the following sections these contents are presented, some of the most important applications of digital watermarking explain some key properties that are desirable in a watermarking system, and also propose a novel approach to position the watermark in the digital image.

II. DIGITAL IMAGE WATERMARKING

Digital watermarking technology, closely related to information security, information hiding, cryptography and authentication technologies, is a cutting edge research area of the international academic research in recent years. In nowadays, the rapid development of network of information and e-commerce make digital watermarking technology very important for all forms of digital products protection, and its application is becoming increasingly widespread. All these set higher demands for people to design a better watermarking algorithm. It must be recognized that digital watermarking technology needs to be combined with these disciplines and technologies so as to resist all kinds of attacks and form integrated solutions for digital products' copyright protection. The demand for this type of technology can be expected to grow enormously as businesses seek to assert some control over their property on the "everything is free" Internet.

Digital image watermarking schemes can be modeled as communication process involving an embedder and detector as depicted in Figure1.

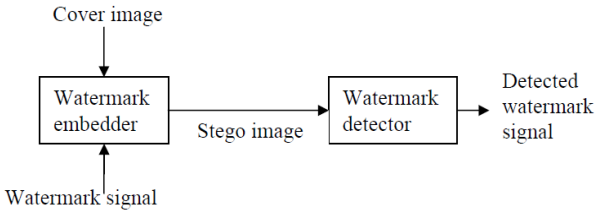

Figure1. A generic watermarking system,

A. Classification of Digital Watermarking

Visible watermark -- The information is visible in the picture. Typically, the information is text or a logo, which identifies the owner of the media.

Invisible watermark -- There is technology available which can insert information into an image which cannot be seen. 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.

Robust watermark -- Embedded invisible watermarks. It resist to image processing or attacks.

Fragile Watermark -- Fragile watermarks are those watermarks which can be easily destroyed by any attempt to tamper with them. Fragile watermarks are destroyed by data manipulation.

Semi Fragile Watermark – These are sensitive to signal modification. Contains feature of both robust & fragile watermark. Provides data authentication.

B. Watermarking properties

Effectiveness -- This is the probability that the message in a watermarked image will be correctly detected.

Fidelity -- Watermarking is a process that alters an original image to add a message to it, therefore it inevitably affects the image's quality.

Payload Size -- Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work.

Robustness -- There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable.

C. Architecture of Digital Watermarking

Watermark embedding embeds the watermark into the original image using a key. The watermark embedding module is as figure1.

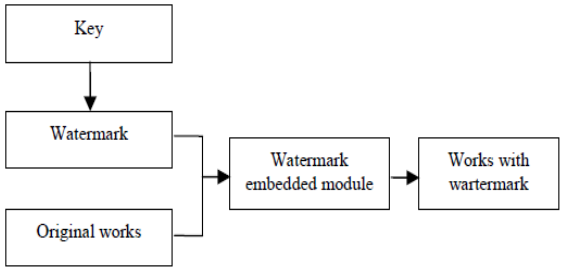

Figure2. Watermark embedding module [1]

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted. The watermark embedding module is as figure 2.

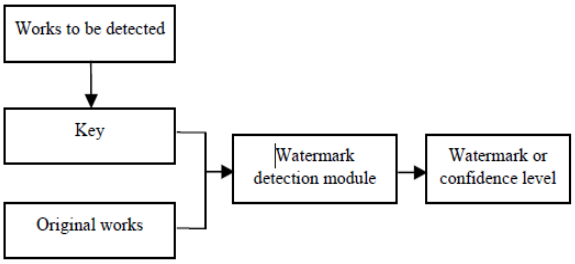

Figure3. Watermark detection and extraction module[1]

D. Watermarking Techniques

There are two major techniques for watermarking –

Spatial Domain – This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels.

Some of its main algorithms are –

Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks.

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.

But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed.

Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

SSM 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.

Texture mapping coding Technique: This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [1], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

Patchwork Algorithm: Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996[11]. 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 where as that of patch B is darkened (for purposes of this illustration this is magnified).

The following are the steps involved in the Patchwork algorithm:

• Generate a pseudo-random bit stream to select pairs of pixels from the cover data.
• For each pair, let d be the difference between the two pixels.
• Encode a bit of information into the pair. Let d < 0 represent 0 and d > 0represent Given that the pixels are not ordered correctly, swap them.
•In the event that d is greater than a predefined threshold or if is equal to 0, ignore the pair and proceed to the next pair.

Patchwork being statistical methods uses redundant pattern encoding to insert message within an image.

Frequency Domain – This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as

Discrete cosine transforms (DCT): DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.

Steps in DCT Block Based Watermarking Algorithm

1) Segment the image into non-overlapping blocks of 8x8
2) Apply forward DCT to each of these blocks
3) Apply some block selection criteria (e.g. HVS)
4) Apply coefficient selection criteria (e.g. highest)
5) Embed watermark by modifying the selected coefficients.
6) Apply inverse DCT transform on each block

Discrete wavelet transforms (DWT): Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, 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. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL).

Advantages of DWT over DCT: Wavelet transform understands the HVS more closely than the DCT.

Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution.

Disadvantages of DWT over DCT: Computational complexity of DWT is more compared to DCT'. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient.

Discrete Fourier transform (DFT): Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

Advantages of DFT over DWT and DCT: DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions.

Table1: Comparison between watermarking techniques

Factors	**Spatial domain**	**Frequency domain**
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational Time	Less	More
Capacity	High	Low
Example of Application	Mainly Authentication	Copy rights

E. Digital Watermarking Applications

Copyright Protection -- Designed to prevent the reproduction of software, films, music, and other media, usually for copyright reasons.

Broadcast monitoring -- With the global television and radio landscape changing more quickly than ever before, how can content owners effectively manage their media assets and ensure fair compensation?

Locating content online -- It has also become a primary sales tool and selling environment, providing an opportunity to showcase our products or services and attract buyers from around the world.

Communication of ownership and copyright -- In our cyber culture, digital has become a primary means of communication and expression. The combination of access and new tools enables digital content to travel faster and further than ever before as it is uploaded, dispersed, viewed, downloaded, modified and repurposed at breathtaking speed.

Content Archiving -- Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video.

Meta Data Insertion -- Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Medical X-rays could store patient records.\

Tamper detection -- Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted.

Digital Fingerprinting -- Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital content. Hence a single digital object can have different fingerprints because they belong to different users.

III. PROPOSED APPROACH FOR WATERMARK POSITIONING

i. Input image is Gray scale image. If in case color image convert it to gray scale image. Approach is for only gray scale image.

ii. Patch is taken and selected (position is fixed and saved) in the image randomly.

iii. Intensity values of the pixels of the image are evaluated.

iv. Threshold value is set using Otsu's method of thresholding.

Otsu suggested a method,
T=graythresh (A);

This method helps in

- Reducing the gray scale image to binary image.
- Image to be thresholded contains two classes of pixels(e.g. Foreground and background)
- Then calculate the optimal threshold separating those two classes so that their combined spread is minimal.

v. Values above the threshold are set to 1 and below are set to 0. Resultant is a binary image, 1 represents white and 0 represents black.

vi. Embedding will be performed only at the white part of the patch in the image i.e. brightness values of the patch in the image.
In case the watermark is big than the space available in the brightness part of the patch selected, then the image segmentation will be performed.

vii. Image segmentation results to several regions/segments in the image. Every segment has two parts black and white part.

viii. Labels are assigned to all the segments in some order.

ix. Now again embedding is performed in the patch's segments including all areas i.e. black and white areas both according to same order as assigned.

IV. CONCLUSION

The purpose of this paper is to present a survey of digital image watermarking approaches and a new novel approach to position the watermark in the digital image in case of space shortage problem. In recent years Digital watermarking has achieved a lot attention. Distribution of movies, music, and images is now faster and easier via computer technology, especially on the Internet. Hence, the content owners are

concerned about illegal copying of their content. Watermarking and cryptography are two standard multimedia security methods. Cryptography does not provide the permanent protection but watermarking does as it provides robustness, invisibility, data capacity and security.

Approach described in this paper in spatial domain provides all the above four properties and provides the strong protection against theft of images over the network.

REFERENCES

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

[2] Ersin ELBAŞI, "Survey on Transformation Based Algorithms in Digital Image Watermarking", 3rd Information Security & Cryptology Conference with International participation.

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

[4] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[5] Zhu, W., Xiong, Z., and Zhang, Y.-Q., "Multiresolution Watermarking for Images and Video", in IEEE Trans. on circuit and System for Video Technology, vol. 9, no. 4, pp. 545-550, June, 1999.

[6] Pereira, S., Pun, T., "Robust Template Matching for Affine Resistant Image Watermarks," in IEEE Transactions on Inage Processing, vol.9, no. 6, pp. 1123-1129, June 2000

[7] "Techniques for data hiding", by W. Bender, D. Gruhl, N. Morimoto, A. Lu

[8] www.networkworld.com

[9] www.digitalwatermarkingalliance.org

[10] www.wikipedia.org

[11] www.scisstudyguides.addr.com

Mr. Prabhishek Singh received his B.Tech in CSE from G.B.T.U Lucknow, Uttar Pradesh, India in 2010.Currently, he is doing M.Tech in CSE from C-DAC Noida(Affiliated to G.G.S.I.P.U New Delhi), India. He is working on the project "**Digital Image Watermarking by Patchwork Method using Image Segmentation**". His interest areas are Digital Image Processing, Operating Systems, and DBMS.

Mr. Ramneet Singh Chadha is an Assistant.Prof, MTech Head and currently working as Project Manager, in Health Informatics group. He has more than 12 years of domain expertise in Health care domain and has been closely involved in Design, Development and Implementation of e-Sushrut HMIS Software, since his joining C-DAC in 1997. He has interest in interoperability of hospitals for setting up NHIN using HL7 standards; cloud computing and telemedicine and other research area is health domain.