Various Authentication Techniques for Watermarking: A Survey

D.Y.Thorat, Shiv K Sahu, Amit Mishra

Abstract-Due to large number of transmission of digital image over non-secure internet, image authentication techniques have recently gained great importance. Digital watermarking is utilized for copy write protection and ownership detection. However as techniques are get improved more focus is given to authentication. Because of authentication digital image become secure and protected to transfer the information over internet. To protect the authenticity of multimedia images different technique has been proposed. These approaches include conventional cryptography, fragile& semi fragile watermarking and digital signature that are based on image content. This paper presents the overview of techniques used for authentication. The different techniques are summarized and compare with each other by considering experimental results.

Keywords: Watermark Lifecycle, Robust Watermarking Schemes, HVS, ICA, Fragile watermarking schemes.

I. INTRODUCTION

The large growth in the digital technology, image processing and Internet has made the reproduction of digitally created information simple and easy. The advancement in World Wide Web, MMS communication has made it possible to transmit and distribute this digitally created information in a fast and easy manner without any quality degradation. Along with some advantage it have important disadvantage of authenticity and protection. Because of this several academicians and researcher work on secrecy of digital image [3]. In schemes have been proposed in the last decade, where a small amount of imperceptible secret information is embedded into the digital content, which can be extracted at a later stage for copyright assertion, copy control, broadcasting, authentication, content integrity verification, etc. [2]. The work on digital Image watermarking is done in regular photo image [6],video[5], audio[4] and the printed material[6],etc. by considering its technical and commercial feasibility. It is a proven method for reducing content piracy and improving the ability to identify tact and manage digital media [7]. It is widely used in applications of rights management, filtering/classification, e-commerce, etc. It is a technique that is used to balance the need for content security with best possible consumer experience to enable media and entertainment industries to adapt the advanced facilities of the modern digital revolution while reducing the threat of content theft.

In [1] watermarking is defined as a technique which embeds data into digital contents such as text, still images, video and audio data without degrading the overall quality of the digital media.

Revised Version Manuscript Received on May 20, 2016.

D.Y.Thorat, M.Tech. Scholar, Department of Information Technology, Technocrats Institute of Technology, Bhopal (Madhya Pradesh). India.

Dr. Shiv K Sahu, Assoc. Prof. & Head, Department of Information Technology, Technocrats Institute of Technology, Bhopal (Madhya Pradesh). India.

Amit Mishra, Asst. Prof., Department of Information Technology, Technocrats Institute of Technology, Bhopal (Madhya Pradesh). India.

A watermark is the data to be hidden and also indicates that the hidden data is transparent, while the term cover media indicates the media used for carrying the watermark. The watermarked information is the media which contains the watermark. In digital watermarking technology, the phrase embedding and extraction means the procedures used for inserting the watermark into the cover media and extracting the embedded watermark from the watermarked data respectively. Detection is process that is used for detecting whether the given media containing a particular watermark.

Digital watermarking techniques originally focused on copyright protection, but have been exploited in wide range of applications [8]. There are number of watermarking schemes that are designed for various applications. Among them, robust watermarks are generally used for copyright protection and ownership identification because they are designed to withstand attacks such as common image processing operations. In contrast, fragile or semi-fragile watermarks are mainly applied to content authentication and integrity attestation because they are fragile to attacks, i.e., it can detect any changes in an image as well as localizing the areas that have been changed. Both these techniques are to be treated separately and this paper deals with Content based watermarking system for authentication. In the paper is organized as below. Section 1 provides an general watermarking systems, Section 2 describes the different types of watermarking. Section 3 shows working based watermarking. A brief conclusion with future direction is presented in Section 4.

II. BASIC WATERMARKING SYSTEM

The basic watermarking system is based on three things Watermark embedding, Watermark Extraction and watermark detection. All these three stages are used in any types of watermarking algorithm.

The block diagram for this is shown in figure 1

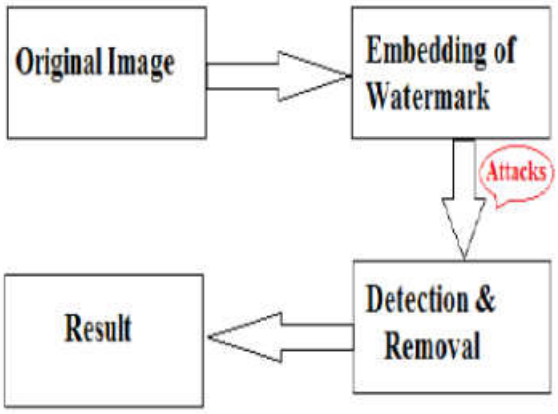


Figure 1: General Watermarking system

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

The given digital watermarking model consists of an embedded and a detector. The embedded takes two inputs. One is the payload we want to embed (the watermark), and the other is the cover work in which we want to embed the payload. The output of the embedder is transmitted or recorded. Later, that Work (or some other Work that has not been through the embedded) is presented as an input to the detector. Most detectors try to determine whether a payload is present, and if so, output the message encoded by it. The watermarking model is analogous to a communication model in which sender encode a message before transmitting it over communication channel and on receiving, receiver decode the encoded message. Here in between the given embedding and detection more chances of attack on the give image. These attacks are of different types shown below:

1) Scrambling Attacks:

This attack is a system level attack in which the part of a Work are scrambled prior to presentation to a watermark detector and then subsequently descrambled.

2) Pathological Distortions:

For a watermark to be secure against unauthorized prevention, it must be robust to process that maintains the fidelity of the Work. Any process may be a normal process, in which case we are requiring that a secure watermark be robust. However, it may also be a process unlikely to occur during the normal processing of the Work. Process that maintains the fidelity of the Work could be used by an adversary to circumvent the detector by masking or eliminating the watermark. the two most common categories of such pathological distortions, geometric/temporal distortions (attacks on synchronization) and noise removal distortions.

- Synchronization Attacks:

Many watermarking techniques are critical to synchronization. By disturbing this synchronization, an adversary attempts to mask the watermark. Examples of simple synchronization distortions include delay and time scaling for audio and video, and rotation, scaling, and translation for images and video. These simple distortions can be implemented such that they vary over time or space. More distortions include pitch-preserving scaling and sample removal in audio, and shearing, horizontal reflection, and column or line removal in images. Even more distortions are possible, such as nonlinear warping of images.

- Linear filtering and noise removal attack:

Linear filtering also can be used by an adversary in an attempt to remove a watermark. For example, a watermark with significant energy in the high frequencies might be degraded by the application of a low pass filter. In any watermarking system for which the added pattern is “noise like” is susceptible to noise-removal techniques.

3) Copy Attacks:

A copy attack occurs when an adversary copies a watermark from one Work to another. As such, it is a form of unauthorized working.

4) Ambiguity Attacks:

Ambiguity attacks create the presence that a watermark has been embedded in a Work when in fact no such embedding has taken place. An adversary can use this dangerous attack to claim ownership of a distributed Work. He or she may even be able to make an ownership claim on the original Work. As such, ambiguity attacks can be considered a form of unauthorized embedding. However, they are usually considered system attacks.

Detection is the process of extraction of given image i.e. we have to separate the original and watermarked image. In this we have to consider the following characteristics so as to find whether any attack is happen or not.

(i) Storage: authentication data should be embedded in the image, such as a watermark, rather than in another file, as is the case with an external signature.

(ii) Mode of extraction: depending on whether authentication data is dependent or not on the image, a full-blind or a semi blind mode of extraction is required. It is quite obvious that a non-blind operation of extraction does not make sense for an authentication service, since the image is necessary.

(iii) Asymmetrical algorithm: contrary to classical security services such as copyright protection, an authentication service requires an asymmetrical watermarking (or encryption) algorithm (i.e., only the author of an image can protect it, but any user must be able to check the content of an image).

(iv) Visibility: authentication data should be invisible under normal observation. It is a question of making sure that the visual impact of watermarking is as weak as possible so that the watermarked image remains faithful to the original.

(v) Robustness and security: it must not be possible for authorize data to be forged or manipulated.

(vi) Protocols: protocols are an important part of any image authentication system, in particular avoid protecting a corrupted picture. The perfect system should have very high capacity, low distortion and high robustness to given attack.

III. DIFFERENT TECHNIQUE FOR WATERMARKING

The watermarking techniques are classified into following categories, namely, Semi-fragile watermarking, Fragile watermarking, robust watermarking, For each technique low embedding space and protection is required, each various category of scheme has different characteristics and, thus, is suitable for different applications. For example, robustness is an important requirement for copyright applications. it has no role in most authentication applications. In this section it gives the different technique given below

3.1. Robust Watermarking

Robust watermarking algorithm aims at mixing a non-perceptible communication channel with image data, in such a way that the capacity of this extra channel degrades smoothly with the distortion the watermarked content undergoes. This class of schemes has verified its applications in so many areas. The numbers of different attacks happen on the digital image are:

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

-JPEG Compression.
- Geometric transform: horizontal flip, rotation, cropping, scaling, deletion of lines or columns, generalized geometrical transformations, random geometric distortions, geometric distortions with JPEG
- Enhancement techniques: histogram modification low pass filtering, sharpening, color quantization, restoration, gamma correction
- Noise addition
- Printing-scanning
- Statistical averaging and collusion
- Over-marking

3.2. Fragile Watermarking Schemes

Most methods currently proposed for providing image authentication are based on a fragile watermark in opposition to robust watermark classically used for copyright protection The basic idea underlying these techniques is to insert a specific watermark (generally independent of the image data [9]) so that any attempt to alter the content of an image will also alter the watermark itself (Figure 2). Therefore, the authentication process consists of locating watermark distortions in order to locate the regions of the image that have been tampered with. The major drawback of these approaches is that it is difficult to distinguish between malicious and non-malicious attacks (e.g., most fragile techniques consider a lossy compressed image as a tampered image, whereas the semantic of the image is unchanged).

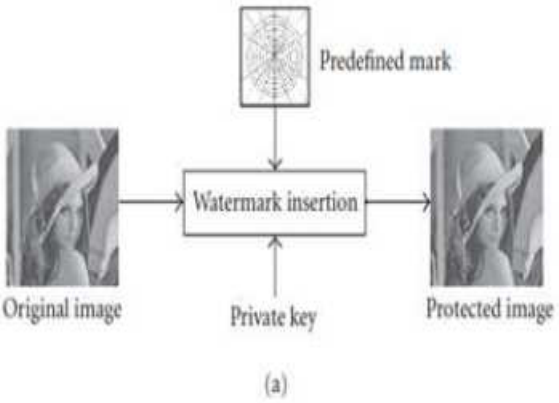
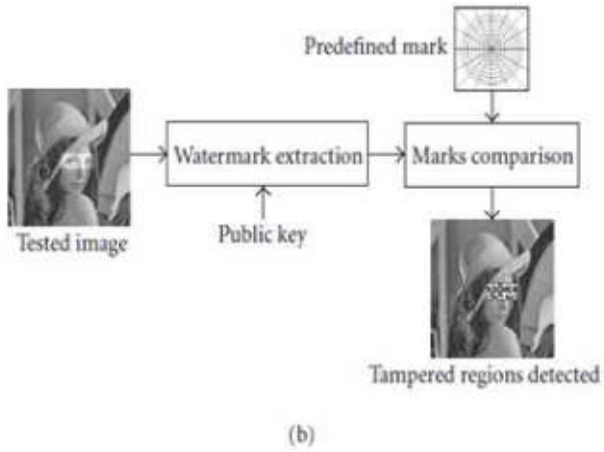


Figure 2: Fragile Watermarking schemes

o Authentication
o Content-integrity verification.

3.3. Semi-Fragile Watermarking Schemes:

A semi fragile watermark is another type of authentication watermark. Fragile watermarks are less robust than fragile watermarks and more sensitive to classical user modifications such as JPEG compression. The aim of these methods is to discriminate between malicious manipulations, such as the addition or removal of a significant element of the image, and global operations preserving the semantic content of the image. The use of this method is mainly justified by the fact that images are transmitted and stored in a compressed form. Moreover, for the most of the applications, the losses due to the



Compression process do not affect the integrity of the image within the meaning of its interpretation.

IV. CONTENT BASED IMAGE WATERMARKING

There are number of techniques available for watermarking for image and video. But we can again have the trouble of authentication. Here we can use the technique of content based watermarking.

4.1. Human Visual System (HVS)

Kay and Izquierdo in [10] used a content based estimation of Just Noticeable Distortion (JND) in frequency domain. To estimate the JND three image characteristics were considered, namely, texture, edginess and smoothness. Their results proved that this technique was resilient to most common attacks like geometric image transformations.

The development and improvement of accurate human vision models helps in the design and growth of perceptual masks that can be used to better hide the watermark information thereby increasing its security. Similarly, in the work proposed by [11], the noise sensitivity of each pixel based on the local region image content such as texture, edge and luminance information was used to obtain the JND mask for the image to be watermarked. Then each bit of the watermark is spread spatially and shaped by pseudo-noise sequence such that its amplitude is kept below the noise sensitive of the pixel into which it is inserted. Experimental results proved that the technique was resistant to compression, cropping and noise attacks.

4.2. Independent Component Analysis (ICA):

DCT and DWT are the two transformation techniques that are widely used in the watermark embedding process. Recently, researchers have started using ICA for watermarking. In ICA was applied to the blocks of the host image and that becomes the watermark. The least-energy independent components of the host were replaced by the high-energy independent components of the watermark image. The drawback of this scheme is that, for watermark extraction both the watermark and the host images are required. This was followed by the work of ,where the host image, the key image, and the watermark image as the independent sources. Embedding was done by weighted addition of the key and the watermark to the host.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

V. CONCLUSION

The above survey gives us the new and innovative techniques of watermarking. Now our research is oriented towards content based watermarking schemes. Most of the proposed watermarking schemes are based on Human Visual System (HVS) using Just Noticeable Distortion (JND) for the selection of watermark positions. ICA a more recent technique is being mainly used for copyright protection.

Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. There is such a strong demand for image manipulation techniques and applications that they are becoming more and more sophisticated and are accessible to a greater number of people. In the current state of research, it is difficult to affirm which approach seems most suitable to ensure an integrity service adapted to images and in a more general way to multimedia documents. There does not exist, any solution perfectly answering this problem.

REFERENCES

1. Steineback, M., Dittann, J. and Neuhold, E. (2009) Digital Watermarking – Common watermarking techniques, Important Parameters, Applied mechanisms, Applications, Invertible watermarking, Content-fragile watermarking, Online Encyclopedia, Contributed Article, http://encyclopedia.jrank.org/articles/ pages/6725/Digital Watermarking.html#ixzz0Zoj226VL
2. [55] Ye, J. and Tan, G. (2008) An Improved Digital Watermarking Algorithm for Meaningful Image, International Conference on Computer Science and Software Engineering, vol. 2, Pp.822-825.
3. [32] Lin, S.D., Kuo, Y. and Huang, Y.(2006) An Image Watermarking Scheme with Tamper Detection And Recovery, First International Conference on Innovative Computing, Information and Control (ICICIC'06), Vol. 3,Pp.74-77.
4. Sachs, D., Anand, R. and Ramchandran, K. (2000) Wireless image transmission using multiple-description based concatenated codes, Proceedings Data Compression Conference DCC 2000, P. 569.
5. Hussein, J. and Mohammed, A. (2009) Robust Video Watermarking using Multi-Band Wavelet Transform, IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1,Pp. 44-49.
6. Kim, Y., Moon, K. and Oh, I. (2003) A text watermarking algorithm based on word classification and inter-word space statistics, Proceedings Seventh International Conference on Document Analysis and Recognition, Pp. 775 -779.
7. Eskicioglu, A. and Delp, E.(2001) An overview of multimedia content protection in consumer electronics devices, Proceedings Signal Processing Image Communication, Vol.16 Ppp. 681-699.
8. Wang, F., Pan, J. and Jain, L.C. (2009) Digital watermarking techniques, Studies in Computational Intelligence, Springer Berlin /Heidelberg, Vol. 232/2009, Pp. 11-26
9. De Strycker, L., Termont, P., Vandewege,J., Haitsma, J., Kalker, A., Maes, M. and Depovere, G. (2000) Implementation of a realtime digital watermarking process for broadcast monitoring on a TriMedia VLIW processor, IEEE Proceedings - Vision, Image and Signal Processing, Vol. 147, No.4, Pp.371-376.
10. Kay, S. and Izquierdo, E. (2001) Robust content based image watermarking, Proc. Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS' 2001, Tampere, Finland.
11. Kay, S. and Izquierdo, E. (2001) Robust content based image watermarking, Proc. Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS' 2001, Tampere, Finland.
12. Ye Xueyi ,ang yunglu ,Zhang jing "A Robust DWT-SVD blind watermarking algorithm based on Zernike moment" ieee 2014 conference communication security
13. Naderahmaderin Y. Beheti .S"Robustness of wavelet domain watermarking against scaling attack"IEEE 2015 international conference on CCECE

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.