REVIEW ON DIGITAL WATERMARKING TECHNIQUE.

Prof.Kavita Ugale,
Assistant Professor,
Department Computer Engg
ISB&M School Of Technology,
Pune, India

Mr.Rohit Lute
Student
Department Computer Engg
ISB&M School Of Technology,
Pune, India

Abstract-Cryptography or cryptology (from greek kryptos, "hidden, secret", and graphein, "to write", or logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead.
In this paper cryptography based Blind image watermarking technique presented that can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks.

IndexTerms–Blind Watermark, Cryptography, Gray scale, Watermarki8ng, Security.

I. Introduction

Digital watermarking studies have always been driven by the improvement of robustness. Furthermore, it is generally impossible to tell whether a given image is authentic or has been altered subsequent to capture by some readily available digital image processing tools. In real life situations, images can be transformed, their pixel values can be modified but not the actual meaning of the image. Security and capacity of watermark data are very important issues to be considered. Watermarking is an emerging research area for copyright protection and authentication of electronic documents and media. Most of the research is going on in this field, spatially in the field of image watermarking. The reason might be that there are so many images available at Internet without any cost, which needs to be protected.

II. OVERVIEW OF DIGITAL IMAGE WATERMARKING:

The digital watermarking is a field of information hiding which hide the crucial information in the original data for protection illegal duplication and distribution of multimedia data. The image watermarking techniques may divide on the basis of domain like spatial domain or transform domain or on the basis of wavelets.

The spatial domain techniques directly work on the pixels and the frequency domain works on the transform coefficients of the image. This paper presents classification of watermarking, stages in watermarking, watermarking approaches and its applications.

1.1 CLASSIFICATION OF WATERMARKING:

A] Visible watermark

Visible watermarking technique generate a visible logo or symbol that clearly seen on watermarked image. This type of watermark used for show the ownership of content like TV channel. Attacking visible watermarking scheme means successfully recover the watermarked area. Implication: Similar image processing techniques can be adopted, Image recovery, object removal.

B] Invisible Watermark

This type of watermark is used to find the ownership as well as prevention from authorized application of image or content. Here, a watermark can insert information into an image which cannot be seen, but can be interrogated with the watermark extraction algorithm. An invisible watermarking process, that stamps a

watermark pattern onto a source image and produces a verification key and a watermark extraction process that decodes the embedded watermark from a stamped image, based on the verification key.

C] Robust Watermark

Robustness watermarking scheme is used for sign copyright information of the digital works, the embedded watermark can resist the common edit processing and various attacks. Digital watermarking is seen as a partial solution to the problem of securing copyright ownership. Essentially, watermarking is defined as the process of embedding sideband data directly into the samples of a digital audio, image, or video signal. Sideband data is typically “extra” information that must be transmitted along with a digital signal, such as block headers or time synchronization markers. It is important to realize that a watermark is not transmitted in addition to a digital signal, but rather as an integral part of the signal samples. The value of watermarking comes from the fact that regular sideband data may be lost or modified when the digital signal is converted between formats, but the samples of the digital signal are unchanged.

D] Fragile Watermark

Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. It can be determined whether the data has been tampered according to the state of fragile watermarking. This work is based on the development of blind fragile watermarking algorithm medical images to grayscale in a wavelet transformed domain. Watermarking is implemented to improve the safety, fidelity, authenticity and content verification images manipulated remotely. The results have been analyzed in terms of imperceptibility and authenticity. Authentication and integrity systems of image can be grouped in several ways depending on the mode of storage of authentication data that is based techniques on electronic signature based or the fragile watermarking or even depending on the nature of the information they burrow into the document to protect.

E] Semi fragile Watermark

Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise compression attacks. Semi-fragile watermark can tolerate “content preserving” operations (such as JPEG compression) and be sensitive to “content altering” transforms (such as feature replacement) is more practicable than fragile watermark in image authentication.

F] Invisible-Robust Watermark

The invisible-robust watermark is embedding in such a way that processes made to the pixel level, which are not determine and it can be recovered only with appropriate decoding process. “Invisible” means that the 2D rendered image of this watermarked volume is perceptually indistinguishable from that of the original volume. "Robust" watermarking implies that the watermark is resistant to most intentional or unintentional attacks.

G] Invisible-Fragile Watermark

The invisible-fragile watermark is embedded in such a way that any attacks of the image would alter or destroy the watermark. The watermarking architecture is prototyped in two ways: (i) by using a Xilinx field-programmable gate array and (ii) by building a custom integrated circuit. This prototype is the first watermarking chip with invisible fragile watermarking capabilities.

2.1 WATERMARKING APPROACHES:

There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

A] Spatial Domain:

Spatial domain digital watermarking algorithms directly load the raw data into

the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image.

B] Frequency Domain:

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients.

3.1 DIGITAL WATERMARKING:

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked

[A] Why Digital Watermarking?

Digital watermarking is an enabling technology for ecommerce strategies: conditional and user specific access to services and resources. Digital watermarking offers several advantages. The details of a good digital watermarking algorithm can be made public knowledge.

4.1 WATERMARK EMBEDDING AND EXTRACTION

A watermark, which is often consists of a binary data sequence, is inserted into a host signal with the use of a key. The information embedding routine imposes small signal changes, determined by the key and the watermark, to generate the watermarked signal. This embedding procedure involves imperceptibly modifying a hoist signal to reflect the information content in the watermark so that the changes can be later observed with the use of the key to ascertain the embedded bit sequence. The process is called watermark extraction.

[A]Watermarks Embedding Procedure

The encryption used in this method is pixel permutation. The operational steps of the watermarks embedding procedure is described below and its block diagram is shown in Figure 1.

[B]Watermarks Extraction Procedure

The extraction procedure is the exact inverse of the embedding procedure. A block diagram of the watermarks extraction procedure is shown in figure.

REFERENCES:

[1] Naina Choubey and Mahendra Kumar Pandey, “Transform based Digital Image Watermarking: An Overview”, in Intl. Jrnl. of Computer Trends and Technology (IJCTT), Vol.24, Number 2, June 2015, pp. 80-83.
CrossRef

[2] Preethi Parashar and Rajeev Kumar Singh, “A Survey: Digital Image Watermarking Techniques”, in Intl. Jrnl. of Signal Processing, Image Processing and Pattern Recognition, Vol.7, No. 6(2014), pp. 111-124.
CrossRef

[3] Prabhishek Singh and R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”, in Intl. Jrnl. of Engineering and Innovative Technology (IJEIT) Vol. 2, Issue 9, March 2013, pp. 165-175.

[4] Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, “A Survey on Watermarking Application Scenarios and Related Attacks”, IEEE international Conference on Image Processing, Vol. 3, pp. 991 – 993, Oct. 2001.

[5] Dr. Martin Kutter and Dr. Frederic Jordan, “Digital Watermarking Technology”, in AlpVision, Switzerland, pp 1 – 4.

[6] Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan, “Hiding Watermark in Watermark”, in IEEE International Symposium in Circuits and Systems (ISCAS), Vol. 4, pp. 4018 – 4021, May 2005.

[7] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, “A Secure Data Hiding Scheme for Two-Color Images”, in Fifth IEEE Symposium on Computers and Communications, pp. 750 – 755, July 2000.