Secure and Authenticated Image Watermarking: A Review

[1]Pridhi Kansal, [2]Sandeep Jain

[1]M.Tech Student, [2]Assistant Professor
Computer Science Department
DVIET, Karnal, Haryana, India
[1]kansal.pridhi@gmail.com, [2] Sandeepjain4891@gmail.com

***Abstract*- Digital watermarking of multimedia content has become a very active research area over the last several years. Watermarking is a very important field for copyrights of various electronic documents and media. With images widely available on the Internet, it may sometimes be desirable to use watermarks. 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. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. This paper proposes a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.**

***Keywords*- Digital Watermark, Steganography, Authentication, Frequency Domain, Spatial Domain, Least Significant Bit**

I. INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. Digital watermarking can be a form of steganography, in which data is hidden in the message without the end user's knowledge. Image watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. A watermark can be classified into two sub-types: visible and invisible. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal, e.g., adding an image as a watermark to another image. Invisible watermarks do not change the signal to a perceptually great extent, i.e., there are only minor variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits. Invisible watermarks that are unknown to the end user are steganographic. Another application is to protect digital media by fingerprinting each copy with the purchaser's information. If the purchaser makes illegitimate copies, these will contain his name. Fingerprints are an extension to watermarking principle and can be both visible and invisible. Figure 1 below shows the general block diagram of watermarking concept.

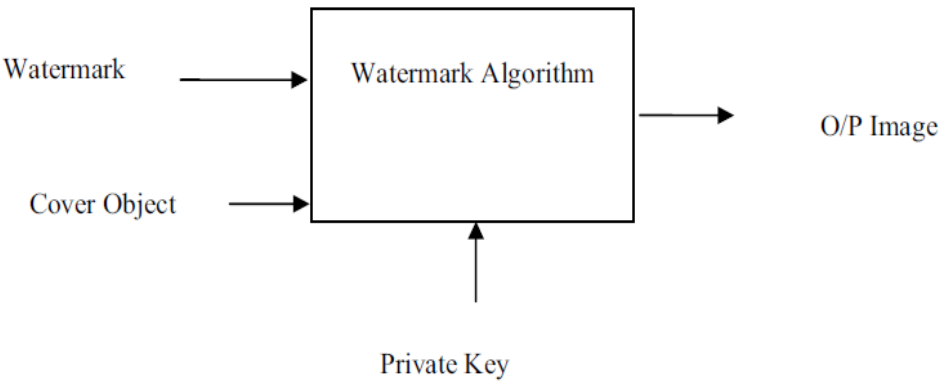

Figure 1 General block diagram of watermarking concept

Although the art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1982, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the moldson which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served as decoration. By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian. They were used as trademarks, to record the date the paper was manufactured, and to indicate the sizes of original sheets. It was also about this time that watermarks began to be used as anticounterfeitinmeasures on money and other documents. The term watermark seems to have been coined near the end of the eighteenth century and may have been derived from the German term wassermarke (though it could also be that the German word is derived from the English). The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was probably given because the marks resemble the effects of water on paper. About the time the term watermark was coined, counterfeiters began developing methods of forging watermarks used to protect paper money.

Counterfeiting prompted advances in watermarking technology. William Congreve, an Englishman, invented a technique for making color watermarks by inserting dyed material into the middle of the paper during papermaking. The resulting marks must have been extremely difficult to forge, because the Bank of England itself declined to use them on the grounds that they were too difficult to make. A more practical technology was invented by another Englishman, William Henry Smith. This replaced the fine wire patterns used to make earlier marks with a sort of shallow relief sculpture, pressed into the paper mold. The resulting variation on the surface of the mold produced beautiful watermarks with varying shades of gray. This is the basic technique used today for the face of President Jackson on the $20 bill. Four hundred years later, in 1954, Emil Hembrooke of the Muzak Corporation filed a patent for "watermarking" musical Works.

Figure 1: Sample picture before Embedding Watermark

Figure 2: Sample picture after Embedding Watermark

II. LITERATURE SURVEY

Many watermarking methods have been proposed in the literature. Schyndel, Tirkel, and Osborne [9] generated a watermark using a m-sequence generator. The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image.The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. Schyndel et al. showed that the resulting image contained an invisible watermark with simple extraction procedures. The watermark, however, was not robust to additive noise.

Cox et al. [10] noted that in order for a watermark to be robust to attack, it must be placed in perceptually significant areas of the image. The watermark was based on 1000 random samples of a N (0, 1) distribution. These samples were added to the 1000 largest.

DCT coefficients of the original image, and the inverse DCT was taken to retrieve the watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient was computed and set to a threshold. If the correlation

was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping, and rescanning. Xia, Boncelet, and Arce [11] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT).

Improvements on the above schemes were possible by utilizing properties of the Human Visual System. Bartolini et al. [12] first generated a watermarked image from DCT coefficients. Then spatial masking was performed on the new image to hide the watermark. Kundur and Hatzinakos [13] embedded the watermark in the wavelet domain.

Bas, Chassery, and Davoine [16] introduced a watermarking system using fractal codes. A collage map was composed from 8x8 blocks of the original image and from the image's DCT. The watermark was added to the collage map to produce a marked image. Results showed that fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique was robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.

III. PROPOSED ALGORITHM

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. This paper proposes a separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data.

Algorithm

- Take the Original image.
- Convert Original image into greyscale.
- Byte conversion of grayscale image.
- Write the certain text to be embedded as watermark in grayscale image.
- Bit conversion of text watermark.
- Byte conversion of text watermark.
- Embedding watermark into grayscale image by using encoding technique.
- Extracting watermark from grayscale image by using decoding technique.

The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version.

When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

IV. METHODOLOGY

A flowchart is a type of diagram that represents an algorithm or process; showing steps as boxes of various kinds, and there order by connecting these with arrows. This diagrammatic representation can give a step by step solution to a given problem. Process operation is represented in these boxes, and arrows connecting them represent flow of control. Flowchart is used in analyzing, designing, documenting or managing process or program in various fields.

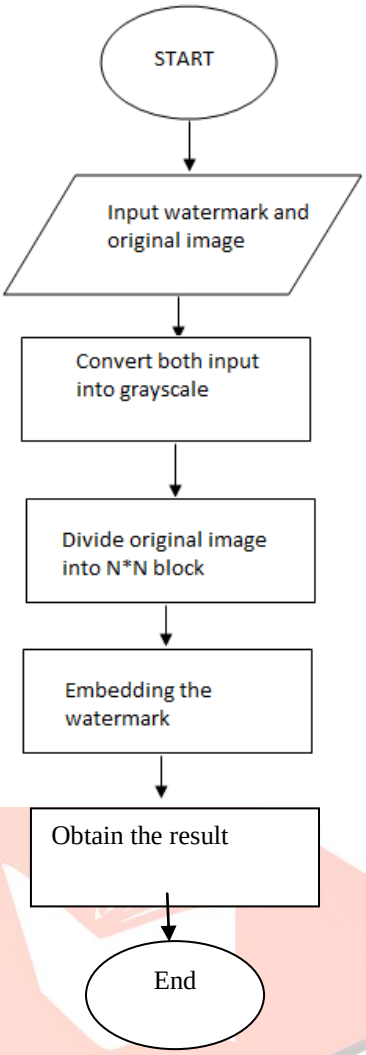

Fig 2 Flowchart

V. OBJECTIVES

The aim of this research is to watermark and dewater mark of images and recover original image even in the presence of noise. There are numerous watermarking methods till date, which can be classified, as described earlier, according to the method of embedding of data inside the medium. All these methods vary mostly in the prospect of providing robustness against attacks, both intentional and unintentional. Here we present two of the most prevalent approaches. The two methods are:

1. **LSB Modification**: One of the most basic techniques of embedding data inside a medium. It involves modification of the LSB of the pixel with the data to be hidden. Although, this approach is not robust to attacks of most of the kinds, it gives a basic overview of the entire watermarking procedure.
2. **Spread-Spectrum Technique**: Recent development in this technique has utilized the concept of Spread-Spectrum technique prevalent in Communications. Arguably, one of the most robust technique, here we consider a new non-linear technique of watermarking.

VI. CONCLUSION

The purpose of this paper is to present a survey of digital image watermarking approaches. The comprehensive review of literature made has uncovered various aspects of Digital Image watermarking.We tried to classify and analyze many previous watermarking methods for the understanding them and a help for new researchers in related areas. We classified the previous works from the various points of view: the inserted media category, the perceptivity, the robustness, the inserting watermark type, the processing method and the necessary data for the watermark extraction. Most of researches handled the watermark techniques on image media. Invisible watermarking, robust watermarking and noise style embedding have been main issues in the previous researches. In terms of processing domain, transform domain has been used rather than the spatial domain. Especially DCT-based approach has been widely used among the transform domain approaches. It is concluded that digital watermarking technique is very impressive for image authentication and for protection against attacks.

REFERENCES

[1] Menezes, A.J., et al., Handbook of Applied Cryptography. 1996: CRC Press. 780 pages.

[2] Cox, I.J., M.L. Miller, and J.A. Bloom, Digital Watermarking. 2002: Morgan Kaufmann.
[3] Geradts, Z.J., et al. Methods for identification of images acquired with Digital cameras. In Enabling Technologies for Law Enforcement and Security. 2001: SPIE.pp.505-512
[4] Liu, K.J.R., et al., Multimedia Fingerprinting Forensics for Traitor Tracing. EURASIP Book Series on SP&C. 2005: Hindawi Publishing Corporation.
[5] Kundur, D. and D. Hatzinakos. Semi-blind image restoration based on telltale watermarking. in Conference Record of the Thirty-Second Asilomar Conference on Signals, Systems & Computers 1998. 1998. Pacific Grove, CA, USA: IEEE.pp.933-937 vol.2
[6] Lin, C.-Y., SARI 1.0: Performance Charts and Technical Description, 2000,online at http://www.ctr.columbia.edu/~cylin/auth/performchart.html, last accessed 11 September 2006
[7] Lin, C.-Y. and S.-F. Chang. SARI: Self-Authentication-and-Recovery Image Watermarking System. in ACM Multimedia 2001. 2001. Ottawa, Canada: ACM Press.pp.628-629
[8] Lyu, S., Natural Image Statistics for Digital Image Forensics, in Department of Computer Science. Ph.D. thesis, Dartmouth College: New York.2005