REVIEW OF IMPERCEPTIBLE TECHNIQUES FOR STILL DIGITAL IMAGE WATERMARKING

Ms. Chandrakala J. Chetri,
Assisstant Professor,
Naran Lala College of Professional & Applied Sciences,
Navsari, Gujarat, India.

Dr. Subhaschandra G. Desai,
Professor,
Sal Institute of Technology & Engineering.,
Ahmedabad, Gujarat, India.

Abstract The purpose of this paper is to explore various techniques used to employ imperceptible watermarking in verification of copyrighted still digital images and evaluate these techniques based on robustness, imperceptibility and computational complexity. The paper focuses mainly on the imperceptible approach for digital watermarking.

Keywords: robust watermark, spatial domain, frequency domain, wavelet transform, imperceptible

1. Introduction

1.1 Watermark

Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. These digital watermarks remain intact under transmission / transformation, allowing us to protect our ownership rights in digital form. In image watermarking, the hidden information is embedded into cover media to prove ownership.

1.2 Digital Watermark

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne [1]. A.Z.Tirkel et al. [1995] discuss the feasibility of coding a robust, undetectable, digital watermark on a standard 512*512 intensity image with an 8 bit gray scale image [2]. J.J.K. O Ruanaidh et al. [1995] discuss the watermarking digital images for copyright protection. They have demonstrated a solution to one of the key problems in image watermarking, namely how to hide robust invisible labels inside grey scale or color digital images [4]. Jian Zhao [1996] describes a digital watermarking service which allows the publisher and information provider to mark and identify their copyrighted materials through the World Wide Web (WWW) [3]. J.J.K. O Ruanaidh et al. [1997] describes an invisible mark embedded in a digital image which may be used for Copyright protection. The embedded marks are designed to be unaffected by any combination of rotation, scale and translation transformations. The original image is not required for extracting the embedded mark [5]. Jian Zhao et al. [1998] describe digital watermark for copyright protection, digital watermark for hidden annotation, digital watermark for proving authenticity,

ISSN: 2278 – 1323

steganographic communication, functions and technical requirements [6].

1.2.1 Stages involved in Digital Watermarking Process

1.2.1.1 Inserting a watermark: - It consists of a watermark insertion unit that uses the original image, the watermark and the user key to obtain the watermarked image.

1.2.1.2 Extracting a watermark: - Extracting the watermark can be divided into two phases, locating the watermark, and recovering the watermark information. Two kinds of extraction are available – using the original document and in the absence of the original document

1.2.1.3 Detecting a watermark: - Consists of an extraction unit to first extract the watermark, and later compare it with the original watermark inserted. The output is Yes or No depending on whether the watermark is present.

2. Types Of Watermarking

2.1 According to the type of data: -
It is divided into four types: image, video, music, text and 3D objects [15].

2.2 According to the working domain: -

2.2.1 Spatial Domain watermarking: - Includes Techniques which directly modifies the intensities of some selected pixels. Watermarking in the spatial domain involves selecting the pixels to be modified based on their location within the image and is very susceptible to cropping and the mosaic attack [16].

2.2.2 Frequency Domain watermarking: - Watermarking in the frequency domain involves selecting the pixels to be modified based on the frequency of occurrence of that particular pixel [18]. This is to overcome the greatest disadvantage of techniques operating in the spatial domain i.e. susceptibility to cropping.

2.3 According to Human Perception: -
2.3.1 Perceptible watermarks: - visible to human eye. They are useful for primary application i.e. for statement ownership or authorship. So for this reason it should be visible [19].
2.3.2 Imperceptible watermarks: - invisible to human eye. They can be detected only by authorized agency. These watermarks are useful for content or author authentication and for detecting unauthorized copier [19].

2.4 According to Robustness: -
2.4.1 Fragile watermarks: - They can be easily destroyed by any attempt to tamper with them. Fragile algorithms aim at discovering and locating the changes introduced in a watermarked picture [8, 9].
2.4.2 Semi-Fragile watermarks: - The aim is to detect and locate the area which has been changed in the watermarked picture [8, 9].
2.4.3 Robust watermarks: - Such watermarks are difficult to remove from the object in which they are embedded, despite various attacks [20].

2.5 According to type of detection: -
2.5.1 Blind watermarking: - This scheme is also known as public watermarking scheme. This is the most challenging type of watermarking system as it requires neither the cover (original data), nor the embedded watermark. These systems

ISSN: 2278 – 1323

extract n bits of the watermark data from the watermarked data (i.e. the watermarked image) [17].

2.5.2 Semi-Blind watermarking: - This scheme is also known as semi-private watermarking scheme. This system does not require the cover (original data) for detection. The purpose of this system to find whether that the watermark can be detected [17].

2.5.3 Non-Blind watermarking: - This scheme is also known as private watermarking scheme. This system requires at least the cover (original data) for detection [17].

3. Techniques For Imperceptible Watermarking

Image watermarking techniques depends on the domain in which the watermarking is done the spatial and frequency domains.

3.1 Spatial Domain watermarking Techniques: - The spatial domain watermarking scheme [16] involves embedding watermarks by directly changing pixel values of host image. Spatial domain algorithms are simple and watermark can be damage easily. It includes techniques which directly modifies the intensities of some selected pixels.

3.1.1 LSB(Least Significant Bit) Technique: - The LSB technique is the simplest technique of watermark insertion [7]. If we specifically consider still images, each pixel of the color image has three components — red, green and blue.

Let us assume we allocate 3 bytes for each pixel. Then, each color has 1 byte, or 8 bits, in which the intensity of that color can be specified on a scale of 0 to 255. Now since each color is stored in a separate byte, the last bit in each byte stores this difference of one. That is, the difference between values 255 and 254, or 127 and 126 is stored in the last bit, called the Least Significant Bit (LSB). Since this difference does not matter much, when we replace the color intensity information in the LSB with watermarking information, the image will still look the same to the naked eye. Thus, for every pixel of 3 bytes (24 bits), we can hide 3 bits of watermarking information, in the LSBs. To extract watermark information, we would simply need to take all the data in the LSBs of the color bytes and combine them.

3.1.2 Block-wise fragile watermarking: - For the purpose of image authentication, our approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed [8]. A block-wise fragile watermarking proposed by Hongjie, et al. (2007) [9] is a standard technique, based on scramble encryption in which the watermark is calculated of all pixels in the whole image. This technique is good enough to localize tampered block but lacks image restoration. This technique will detect altered block as well as restore it with good approximation without changing the present working domain that is spatial domain.

3.1.3 Cryptography image watermarking: - Images can be encrypted in their source codes for safe transmission. Here the research deals with image encryption and watermarking. There are several methods to encrypt binary or gray level images [10, 11]. An idea is to apply reversible lossless data hiding algorithms on image before encryption is done, So that security level is also high [12, 13].

ISSN: 2278 – 1323

Image Watermarking using Least Significant Bit (LSB) method [14] has been used for embedding the information. In this method the original image is embedded with watermark image before encryption by using lossless watermarking method & encryption algorithm is applied for encryption of embedded image using private key. The watermarking objective is to embed invisibly message inside the image.

3.2 Frequency Domain watermarking techniques: - The frequency domain technique transforms an image into a set of frequency domain coefficients [18]. It involves selecting the pixels to be modified based on the frequency of occurrence of that particular pixel. The image is segmented into multiple frequency bands [19]. After applying transformation**,** watermark is embedded in the transformed coefficients of the image such that watermark is not visible [20]. Finally, the watermarked image is obtained by acquiring inverse transformation of the coefficients.

3.2.1 Matrix encoding technique: - Secure data will be stored in last 3 bits of each smaller segment separately. The data is store on the high intensity pixel frequency of LSB [21] in each area. The Capacity of text embedding depends upon image size. After calculating the capacity of given text multiple text file can be add into the image [22]. Security is being increased by selection of random image segment to store the data behind the segment of image [23]. The selection of random segment is done by using random generator function. Selection of random segments for hiding the data makes impossible for intruder to reveal the data until they do not know where the data is hiding.

3.2.2 DWT based watermarking scheme: - DWT decomposes image hierarchically, providing both spatial and frequency description of the image [24]. In this scheme, the transformation adopted is Discrete Wavelet Transforms (DWT). Yuan et al. (2006) [25] proposed an integer wavelet based Multiple logo watermarking scheme. The watermark is permuted using Arnold transform and is embedded by modifying the coefficients of the HH and LL subbands. Qiwei et al. (2009) [26] put forward a DWT based blind-watermarking scheme by scrambling the watermark using chaos sequence. After applying transformation, watermark is embedded in the transformed coefficients of the image such that watermark is not visible. Finally, the watermarked image is obtained by applying inverse transformation of the coefficients. Proposed watermarking scheme extracts and generates watermark information from watermarked image and so original image is not essential. So it can be referred as blind watermarking.

3.2.3 Robust Image Watermarking: - For a digital watermark to be effective for ownership assertion, it must be robust [20], recoverable from a document, provide the original information embedded reliably, be non-intrusive, and also removable by authorised users.

With regard to still images that consist of a two-dimensional signal, it is to be decomposed into DWT pyramid structure with various frequency bands. G. Dayalin Leena et al. (2013) [27] proposed system that is effective and securely embeds a color carrier image with a color watermark. Carrier image is separated into R, G, B component where each of separated component forms gray images. The

ISSN: 2278 – 1323

watermark taken is resized by removing the unwanted pixels if any. Resizing is purely depending on the final decomposed level of carrier image. Arnold's cat map transform is applied on the rescaled watermark in which the watermark now becomes a chaos of pixels instead of a proper image. Arnold Transform, known as "cat face transform", is a pixel position transformation proposed by Vladimir Arnold when he studied argotic theory. Arnold Transform changes the pixel location of the image by matrix operations. So the shuffled watermark is embedded with the last decomposed level of original image. Embedding technique is applied for the entire three separated component. By applying inverse discrete wavelet transform (IDWT) on each of the embedded image coefficients and merging the three embedded image coefficients, the watermarked image is produced.

4. Comparison Of Various Techniques

Various methods for invisible watermarking proposed possess merits & demerits. The selection of an appropriate technique will base on various factors like robustness, imperceptibility & better quality.

4.1 Robustness: - The technique should tolerate some of the common image processing attacks. Watermark is called robust if it resists a designated class of transformations. Spatial domain techniques are very susceptible to cropping and the mosaic attack. So they are less robust compared to frequency domain techniques. Frequency domain algorithms can resist various intensity attacks and watermark information cannot be damaged easily. Frequency domain techniques embeds & extracts watermark into low-level or medium-level frequency bands which prevents the watermarked image being destroyed due to compression methods. Also the watermark is dispersed throughout the original image so very less susceptible to cropping attacks.

4.2 Imperceptibility: - A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un-watermarked content. Spatial domain techniques tend to modify the pixels of the original image directly which might create degradation of the watermarked image from the original image. Frequency domain techniques performs embedding of watermark image in transformed version of the image, the alteration is less noticeable to the human eye. Hence the watermarked image is undistinguishable from the original one.

4.3 Better Quality: - During the generation of the watermarked image, the degradation of the quality should not be reflected. It must maintain better contrast of the image. In spatial domain, luminance values of original image are altered in order to hide a watermark. Mostly, LSB technique replaces the original image with bits of watermark. But this approach falls down whenever there is a need to hide large number of bits in an image. If large numbers of bits are modified in the original image, the pixel dependency will fail to produce an efficient watermarked image. This issue has been dealt well by frequency domain techniques. The reason is that the characteristics of the human vision system (HVS) are better captured by the spectral coefficients.

ISSN: 2278 – 1323

5. Conclusion

Digital images can be watermarked either in spatial domain or in frequency domain. The goal is to produce an efficient, secure and invisible watermarked image using digital watermarking thereby improving the quality and increasing the robustness of watermarked image. Image robustness must be checked well by including attacks and extracting the watermark from the attacked watermarked image without any quality degradation in the original image. The technique is expected to achieve high robustness against various intensities attacks and maintaining imperceptibility of the watermarked image from the original one. My insight of research work will be to overcome all the issues of various techniques. My major focus will be towards achieving imperceptibility with high robustness.

References

[1] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Watermark", DICTA 93, Macquarie University. pp. 666-673, (1995).

[2] A.Z.Tirkel, R.G.van Schyndel, C.F.Osborne, "A TWO-DIMENSIONAL DIGITAL WATERMARK", DICTA 95, Macquarie University, (1995)

[3] Jian Zhao, "A WWW SERVICE TO EMBED AND PROVE DIGITAL COPYRIGHT WATERMARKS",In: Proc. of the European Conference on Multimedia Applications, Services and techniques, Louvain-La-Neuve, Belgium, May, (1996).

[4] J.J.K. O Ruanaidh,W.J. Dowling, F.M. Boland,"Watermarking Digital Images for Copyright Protection", IEEE, (1995).

[5] Joseph J.K. O Runaidh and Thierry Pun, "Rotation.Scale and Translation Invarient Digital Image Watermarking", Submitted to Signal Processing,21 August, (1997).

[6] Jian Zhao, Eckhard Koch, and Chenghui Luo, In Business Today and Tomorrow, COMMUNICATIONS OF THE ACM July 1998/Vol. 41, No. 7, (1998).

[7] C.I.Podilchuk, and E.J.Delp, "Digital watermarking: algorithms and applications", IEEE Signal Processing Magazine, pp. 33-46, (2001).

[8] Chun-Shien Lu and Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, pp.1579-1592, (2001).

[9] He Hongjie, Zhang Jiashu and Chen Fan, "Block-wise Fragile Watermarking Scheme Based on Scramble Encryption", IEEE 978-1-4244-4105-1/07, (2007).

[10] C-C Chang, M.S. Hwang, and T-S Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software, 58, PP.83–91, (2001).

[11] W. Puech. "Image Encryption and Compression for Medical Image Security" proceeding of IEEE Image Processing Theory", Tools & Applications, (2008).

[12] Xinpeng Zhang]ieee signal processing letters, "Reversible Data Hiding in Encrypted Image", vol. 18, no. 4,pp.255,(2011).

[13] W. Puech, M. Chaumont, and 0. Strauss, "A Reversible Data Hiding Method for Encrypted Images", In Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia

ISSN: 2278 – 1323

Contents X, volume 6819, pp. 68191E-1-68191E-9, (2008).

[14] H. Farid, "Detecting hidden messages using higher-order statistical models", Proceeding of IEEE, vol. 15, no. 6 , pp. 68-72, (2002).

[15] Authors Emir Ganic, Ahmet M. Eskicioglu, "Robust DWTSVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Magdeburg, Germany, pp. 166 - 174, (2004).

[16] FrankY. Shih, Scott Y.T. Wu, "Combinational image watermarking in the spatial and frequency domains",Science Direct, Vol. 36, No. 4, PP. 969-975, (2003).

[17] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, pp. 133-144, (2004).

[18] Frank Hartung, Martin Kutter,"Multimedia Watermarking Techniques", Proceedings of IEEE, Vol. 87, No. 7, pp. 1085 – 1103, (1999).

[19] Yongjian Hu, Sam Kwong and Jiwu Huang,"Using Invisible Watermarks to Protect Visibly Watermarked Images", Vol.5, PP. 584- 587, (2004).

[20] Cox, I. J., J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol.6, no.12, pp.1673-1687,(1997).

[21] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit", journal of computing, Vol. 3, issue 4, (2011).

[22] XIE Qing, XIE Jianquan, XIAO Yunhua "A High Capacity Information Hiding Algorithm In Color Image" IEEE ,(2010).

[23] Sabyasachi Samanta, Saurabh Dutta, Goutam Sanyal "An Enhancement of Security of Image using Permutation of RGB Components" IEEE, (2011).

[24] Vaishali S. Jabade,Dr. Sachin R. Gengaje, " Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications (0975 –8887) , Volume 31– No.1, pp. 28-35, (2011).

[25] Yuan Yuan, Decai Huang, and Duanyang Liu, An Integer Wavelet Based Multiple Logo-watermarking Scheme. In IEEE, Vol.2 pp.175-179, (2006).

[26] Qiwei Lin, Zhenhui Liu, and Gui Feng, "DWT based on watermarking algorihthm and its implementing with DSP", IEEE Xplore, pp. 131-134, (2009).

[27] G. Dayalin Leena and S. Selva Dhayanithy(2013), "Robust Image Watermarking in Frequency Domain", International Journal of Innovation and Applied Studies ISSN 2028- 9324 Vol. 2 No. 4 , pp. 582-587, (2013).

ISSN: 2278 – 1323