Volume 2, No. 8, August 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
TECHNICAL NOTE
Available Online at www.jgrcs.info

IMAGE WATERMARKING: A SURVEY

Sirsendu Sarbavidya[*1], Sunil Karforma[2]
*[1]Lecturer, Department of Computer Science & Technology
Kanyapur Polytechnic, Asansol – 5, Burdwan, India sirsendusarbavidya@gmail.com[1]
[2]Reader, Department of Computer Science University of Burdwan, Burdwan, India
sunilkarforma@yahoo.com[2]

Abstract: To provide ownership of media and to protect it from unwanted changes, encryption & control access techniques were used in earlier days. But, with the advancement of digital communication and easy availability of cheap recording and storing devices, the security of digital information is under threat. Any one can easily obtain, replicate and distribute digital image without any loss in quality. Therefore, we need to develop a system that can not only prevent unauthorized access of the content but also help to establish ownership rights, content authentication and prevent illegal replication. In order to successfully implement all these, watermarking is used globally. Watermarking is a technique for embedding additional data which is used for copyright protection and ownership identification. The embedded watermark should be robust enough to survive all sorts of attacks. This paper conducts a literature survey of existing & newly proposed watermarking techniques along with their potential application areas.

Keywords: Digital Watermarking, Image-dependent Watermarking, Content Security, Half-toned Image, Lapped Orthogonal Transform, Pdf-Matched Embedding.

INTRODUCTION

With the exponential growth of computer network industry and easy availability of large volume of information, a problem related to information security has generated. In modern days, generally information's are available in digital form and anyone can make a perfect copy of the information very easily without generating any changes to the original content. To restrict this kind of practice and to help protect the integrity and authenticity of the content as well as the copyright ownership, researchers have developed innovative methods for secret communication, called watermarking.

HISTORY

Digital watermarking is a technique to insert a digital signature into the content so that the signature can be extracted for the purposes of ownership verification and/or authentication. The term watermark has been derived from the German term *wassermarke* [3], which resembles the effect of water on paper. The oldest watermark was found in a paper originated in the town of Fabriano in Italy in the year 1282 [3]. The introduction of watermark within the paper helps to identify ownership among the papermaking industry [4]. In the year 1887 in France, two watermarked letter helps to solve a prosecution case. William Congreve, an Englishman, invented a technique for paper watermarking by inserting dyed material into the middle of the paper at the time of producing the paper [3]. Another Englishman, William Henry Smith was developed a method of paper watermarking by pressing the paper mold with a sort of shallow relief sculpture [3]. Paper watermarks are extensively used in bank notes and stamps nowadays. In 1954, Emil Hembrooke of Muzak Corporation has designed a technique to watermark musical property [3]. In 1979, Szepanski developed a watermark pattern for anti-counterfeiting and in the late 1980's, there evolved a term called digital watermarking analogues to the paper watermarking. In the year 1986, Holt et al. described a watermarking method for audio signal [3]. In the year 1988, Komatsu and Tominga, first coined the term *digital watermark* in their works. Since 1995, digital watermarking has gained a lot of attention from researchers as well as from several different organizations and growing very rapidly [4]. In the year 1996, digital watermarking gets its first global acceptance when they are included as one of the primary topics in the Information Hiding Workshop (IHW) [3].

BASIC PRINCIPLES

All watermarking applications share two principle ideas: a watermark embedding method and a watermark recovery method.

In watermark embedding process [4, 5], the input to the scheme is the watermark, the cover-media and a key. The key is used to enforce security, which is the prevention of unauthorized parties from recovering and manipulating the watermark. The output of the watermarking scheme is the watermarked data. The generalized watermark embedding function is $E_k(I,W) = I'$

In Watermark detection process [4, 5], inputs to the scheme are the watermarked data, key, and the original watermark. The output of the scheme gives us some kind of confidence measure indicating whether the test data is authentic or not. The generalized watermark recovery function is $D_k(I'',W) = 1/0$.

APPLICATIONS

In this portion of the text, we are concentrating only on the application domain of the digital watermarking. The application of digital watermarking covers a large portion of the content protection. We survey papers, related to the protection of image using digital watermarking. Watermarking is employed in various useful applications. They are attractive for signals consisting of continuous stream such as audio and video [2, 5]. To protect intellectual

property, watermarking is a very helpful weapon for the individual as well as the industry. In intellectual property protection, we need to deal with two aspects. The first one provides protection against misappropriation of creations by others and the second one provides protection against unauthorized use. It is also used in the X-ray photography [2, 5] for testing and documenting the structural integrity of buildings and materials. In some playback device that contains embedded subsystem within it, fingerprint watermark helps to identify the rights verification of the system. In the recent years, watermarking has been extensively used to support multimedia contents. Broadcast monitoring is another area of application where watermarking is proven to be helpful in protecting the interest of the advertiser as well as the broadcaster. Another well known application of the watermark is in the field of transaction tracking. Using embedded watermark, authenticity of the content is also proved. In the copy control application, the embedded watermark prevents user from making illegal copies. With the help of modern watermarking methods, a user can restrict and control the use of any device that supports the technique. Digital watermarking is one of the ways via which legacy enforcement are performed.

REVIEW ON RECENT METHODS

This section attempts to provide a highlight regarding the most important image watermarking applications in recent pasts.

A. The survey of Rey et al. [6] identifies some of the emerging techniques of that time. They introduced the notion of image content authentication so that they can easily detect image tampering. They also highlighted the features about effective authentication scheme. They proposed an approach using feature based watermarking to show that an image is authentic even though the content has been modified.

B. Caldelli et al. [7] in their paper proposed a digital watermark solution for authentication of remote-sensing images. They used standard JPEG-LS algorithm for near lossless compression. Here, the authentication is carried out with the help of near-lossless coding. Here, image integrity can be tested with the help of known secret key. This paper identifies that one can apply watermarking into individual blocks also. Thus the approach support robust watermarking. The algorithm proposed in the paper does not produce better result with respect to tamper localization and each reconstructed pixel can differ from the corresponding original pixel by an amount bigger than the maximum error preset in the algorithm.

C. In this paper, Hien et al. [8] proposed a new robust logo watermarking technique. Here, watermark embedding is performed in the wavelet domain of the host image. Independent Component Analysis (ICA) is introduced here to extract the logo watermark. ICA is used here to extract original watermark that was hidden in the image. The proposed algorithm is based on blind image watermarking and can survive under almost all compression domains. The proposed method can survive in various types of attacks, such as cropping of an image, low-pass and median filtering, adding noise, image resizing etc.

D. In this paper, Braudaway et al. [9] proposed a method to place one or more watermarks into a printed page composed of unmarked and previously half-toned sub-images and to successfully detect the inserted watermark from a scan of the printed page. They begun the process by inserting an invisible watermark into a uniform white digitized image. After that they convert the digitized image by a half-toning method into a foundation and then overlaying one or more previously half-toned sub-images onto the foundation to form a printable image. Here, each sub-image is produced using either same or different halftone method depending on the content. The preparation of half-tone images generates high energy high frequency noise and makes watermark detection more difficult.

E. Xu et al. [10] presented a hybrid image protection scheme to establish a relationship between the data encryption key and the watermark. They used the activating share to carry the copyright information. They also embed the bit stream, representing the data, into the content to provide visual watermark. The change in encryption key also generates change in activating share and thus changes the corresponding watermark information. Before transmission, the stream is encrypted via encryption key and at the time of receiving, decryption is carried out by regenerating the same key that extract the watermark from the image. The proposed method can be easily used in unicast, broadcast and multicast applications of multimedia. Here, encryption is used to prevent unauthorized access to multimedia content and watermarking is used for copyright protection. The proposed scheme used preposition secret sharing for the construction of fresh encryption keys.

F. Lichtenanuer et al. [11] proposed a possible solution of geometrical distortion of watermarked images in this paper. They used a template grid in the autocorrelation function. Their proposed solution modulates the watermark with a pattern derived from the image content and the secret key. The hidden watermark pattern makes malicious attack difficult but the time requirement for pattern generation is very high. They used frequency domain filtering for hiding the information. They applied template hiding by secret modulation and make the watermark template robust by adjusting cropping.

G. Liu et al. [12] proposed a robust, invisible watermarking scheme for digital images in this paper. Here, the watermark is embedded using the block-based Lapped Orthogonal Transform (LOT) and it follows a spread spectrum watermarking approach. It allows larger watermark embedding energy but preserves invisibility intact. They used human visual system (HVS) model to adjust the energy of the watermark during embedding. Here, each block is categorized into one of four classes (texture, fine-texture, edge, and plain-area) and they follow Texture Masking Energy (TME) approach. The scheme used here is known as LOT based adaptive image watermarking.

H. Liu et al. [13] proposed a pdf-matched embedding (PME) scheme in this paper. They generalized the PME

scheme by considering the probability distribution of host image and then constructing a pdf-matched quantizer as the starting point. The generated pdf-matched quantizer is robust against attacks and produces better result when distortion caused due to embedding and also enhances embedding capacity. They further decrease distortion embedding by using vector flipping and DC-PME. Their proposed approach performs better than the uniform quantizer based schemes. They showed that for higher dimensions and vector bit embedding the performance can be improved further.

I. In this paper, Seo et al. [14] proposed a method for content based watermarking based on feature points of an image. They embed watermark at each and every feature point after affine normalization according to the local characteristic scale. The proposed approach is robust enough against cropping, filtering, and affine normalization and JPEG compression. It also supports resilience against geometric distortions in watermark detection. Here, the original image is not needed for the watermark detection. In this paper, the inaccuracy of feature point is overcome by using the local search. The proposed method is computationally demanding than normal watermarking and can easily handle geometric distortions.

J. Pla et al. [15] proposed a technique that constructs an image-dependent watermark in the discrete wavelet transform (DWT) domain and inserts the watermark in the most significant coefficients of the image. They used hierarchical tree structure to determine the watermark coefficients and if any attack appears on the watermarked image, the tree structure allows the correlation based watermark detector to recover synchronization. They used visual adaptive scheme to insert the watermark and a template is inserted into the watermark to provide robustness against geometric attacks. The watermark is robust against JPEG compression, median filtering, and sharpening.

K. Fridrich et al. [16] proposed a lossless watermarking technique that preserves the file size. They have chosen two file formats – RLE encoded bitmaps and sequentially encoded JPEG images. The embedded message and the exact copy of the original image can be obtained after the image is decompressed, re-encoded, when its palette is permuted or colors added to it.

L. In this paper, Leest et al. [17] proposed a general framework for reversible watermarking in multi-media signals. A mapping function is used to map the input signal to a perceptually equivalent output signal. The unused sample values of the output are used to encode watermark information and restoration data. They increase the dynamic range of the image to produce extra space for embedded information. They allow perceptual distortion and via contrast enhancement embedding they obtain high capacity of embedding information.

M. In this paper, Stach et al. [18] proposed a high capacity, data hiding algorithm that lets the user restore the original host image after retrieving the hidden data. The algorithm follows generalized, reversible, integer transform, which calculates the average and pair wise difference between the elements of a vector extracted from the pixels of the image. The watermark bit is embedded by replacing the LSB of every selected coefficient. The coefficient selection ensures that the embedding process does not cause any overflow or underflow when the inverse transformation takes place. The locations of the shifted coefficients and the original LSBs are embedded in the selected coefficients to support method of reversibility. The algorithm allows the user to recover the original host image after retrieval of hidden data.

N. Yang et al. [19] proposed a high capacity reversible watermarking scheme using companding technique over integer DCT coefficients of image blocks. They have chosen AC coefficients in the DCT domain for the bit-shift operation. They choose different numbers of coefficients of different frequencies to maintain capacity and quality of the watermarked image. They used block discrimination structure to find suitable blocks that can be used for embedding but that does not generate any overflow or underflow. The watermark information can be extracted correctly without making any change to the original image. The value modification caused by the bit-shift operation is one of the major drawbacks of the proposed algorithm.

O. In this paper, Katzenbeisser et al. [20] characterize and analyze possible malicious attacks against watermark based image authentication systems and also identifies security measurement criteria. With respect to media authentication schemes, they identified – attacks against the key distribution, attacks against the integrity test, and attacks against secrecy and integrity of the original. To protect the original image they has designed a secret session key and the condition that guided the use of key is that it should not be used twice.

P. Desurmont et al. [21] proposed a robust image watermarking algorithm for discouraging illicit copying and distribution of copyright material. They add synchronized information to counter the problems generated by geometric distortions. Here, they present an analysis of this type of distortions and proposed a metric to estimate the distortion of an image. The metric is content independent and invariant to global translation, rotation, and scaling.

Q. Wang et al. [22] specified, a wavelet based watermark casting scheme and a blind watermark retrieval technique, in this paper. At first they determine significant wavelet sub-bands and then select a couple of significant wavelet coefficients in the generated sub-bands so that a watermark can be easily embedded. Here, they proposed a perceptual watermark casting scheme that searches the perceptually significant coefficients to provide a higher tolerance to avoid attacks. They can easily adjust the fidelity of the watermark sequence by using weighting factor for watermark energy.

R. In this paper, Wong et al. [23] proposed a public key watermarking algorithm for image integrity verification. The watermark can easily identify changes in pixel values and image sizes. The watermark extraction can be performed with the help of public key and can be performed by any person without having exchanging secure information with the other party.

S. Jumma et al. [24] proposed a watermarking method to protect digital images from illegal manipulation using Discrete Wavelet Transform and Discrete Cosine Transform. They has designed a method, to meet imperceptibility, robustness and security requirements, based on peak signal to noise ratio and bit correct ratio measurements.

T. In this paper, Iovane et al. [25] proposed a new highly performing system to establish the Intellectual Property of a file by using advanced Information Fusion techniques based on face biometrics and wavelet multi-resolution analysis. Based on types of information available, the proposed approach use different watermarking schemes and can be useful for all types of files distributed online. They also provide information regarding information entropy to track the access and use of a specific file by different users.

CONCLUSIONS

This paper presented a background discussion on the major application area of image watermarking. We have chosen research papers from last 20 years and wanted to draw a conclusion about how the progress are going on in the corresponding field of research. Though variety of approaches has been discussed in the literature, most approaches are not secure against all kinds of attack. It is really impossible for a single approach to satisfy all sorts of parameters. So, selection of any particular approach totally depends upon the actual requirement of the application. We can conclude that the challenge of the researcher is to develop an approach which will satisfy all the requirements of each and every application.

REFERENCES

[1]. A. Cheddad, J. Condell, K. Curran, and P. Mckevitt, Digital Image Steganography: Survey and Analysis of current methods. http://isrc.ulster.ac.uk

[2]. E. H. Fu, Literature survey on Digital Image Watermarking, EE381K, Multimedia Dimensional Signal Processing, 1998. http://

[3]. J. J. Cox, M. L. Miller, J. A. Bloom, J. K. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann Publishers, 2nd Edition, 2003.

[4]. S. Katzenbeisser, and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston, USA, 2000.

[5]. M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermarking and Content Protection, Artech House, Boston, USA, 2003.

[6]. C. Rey, J.L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing 2002:6, pp. 613 – 621, Hindawi Publishing Corporation.

[7]. R. Caldelli, G. Macaluso, F. Bartolini, M. Barni, "Near Lossless Image authentication Transparent to near Lossless Coding", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 737 – 747.

[8]. T.D. Hien, Z. Nakao, Y.W. Chen, "ICA based robust Logo Image Watermarking", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 162 – 172.

[9]. G.W. Braudaway, F. Mintzer, "Application of Invisible Image Watermarks to previously halftoned images", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 663 – 669.

[10]. X. Xu, S. Dexter, A.M. Esticioglu, "A Hybrid Scheme for encryption & watermarking", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 725 – 736.

[11]. J. Lichtenauer, I. Setyawan, R. Lagendijk, "Hiding Correlation Based Watermark Templates using Secret Modulation", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 501 – 512.

[12]. Y. Liu, B. Ni, X. Feng, E.J. Delp, "LOT Based Adaptive Image Watermarking", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 513 – 523.

[13]. N. Liu, K.P. Subbalakshmi, 'Vector Quantization Based Scheme for Data Embedding for Images", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 548 – 559.

[14]. J.S. Seo, C.D. Yoo, "Image Watermarking based on scale space representation", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 560 – 570.

[15]. O.G. Pla, E.T. Lin, E.J. Delp, "A Wavelet Watermarking algorithm based on a Tree Structure", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 571 – 580.

[16]. J. Fridrich, M. Goljan, Q. Chen, V. Pathak, "Lossless Data Embedding with File size Preservation", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 354 – 365.

[17]. A.V. Leest, M.V.D. Veen, F. Bruekers, "Reversible Watermarking for Images", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 374 – 385.

[18]. J. Stach, A.M. Alattar, "A High Capacity, Invertible, Data Hiding Algorithm using a Generalized, Reversible, Integer Transform", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 386 – 396.

[19]. B. Yang, M. Schmucker, W. Funk, C. Busch, S. Sun, "Integer DCT bsed Reversible Watermarking for Images using Companding Technique", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 405 – 415.

[20]. S. Katzenbeisser, J. Dittmann, "Malicious Attacks on Media Authentication Schemes Based on Invertible Watermarks", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 838 – 847.

[21]. X. Desurmont, J.F. Delaigle, B. Macq, "Characteristics of Geometric Distortions Attacks in Robust Watermarking", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 870 – 878.

[22]. H.J.M Wang, P.C. Su, C.J. Kuo, "Wavelet based digital image watermarking", 7 dec, 1998 / vol. 3, No. 121, OPTICS EXPRESS 491.

[23]. P.W. Wong, "A Public key watermarking for Image Verification & Authentication", 1998, IEEE.

[24]. P.W. Wong, "A Public key watermarking for Image Verification & Authentication", 1998, IEEE.

[25]. Jumaa B. A., Aladdin A., "Image Watermarking using DWT-DCT", Engineering & Technology Journal, Vol. 28, No. 23, 2010.

[26]. Iovane G., Giordano P., Borysenko S. D., "Image Watermarking via wavelet approach & face biometrics", Journal of Ambient Intelligence and Humanized Computing.

