www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 03 Issue 07 July, 2014 Page No. 7084-7087

Survey: Digital Image Watermarking Technique

Aditya Bhagat, Shikha Singh
Dr. C.V. Raman University
Bilaspur, India
rajeaadi@gmail.com
Asst professor
Dr. C V Raman University
Bilaspur India
shikha.mishra687@gmail.com

***Abstract*—The "Digital Image Watermarking" is the process of embedding information into a digital media without compromising the media's value in a way that it is difficult to remove. This is basically used to hide the information from attackers.**

1. DATA HIDING

Data Hiding is a process to hide a data from attackers. Data Hiding should be done through a various methods.

1.1. HISTORY OF DATA HIDING

Data Hiding has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, data hiding is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. This chapter will explore data hiding from its earliest instances and watermarking as its present potential application. The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the west appears in Homer's Iliad. Steganographic method made their record debut few centuries later in several tales by Herodotus, the father of history. An important technique was the use of sympathetic inks. Later chemically affected sympathetic inks were used. This was used in World War 1 and 2. The term steganography came into use in 1500's after the appearance of Trithemius' book on Steganographia, semagram, and open code. Semagram is secret message not in written form.

Watermarking has evolved from Steganography. Watermarking is as old as paper manufacturing. Today most developed countries watermark their paper, currencies and postage stamps to make forgery more difficult. The digitization of the world has expanded the watermarking concept to include immaterial digital impressions for use in authentication ownership claims and protecting proprietary interests. Watermarking gives guarantee of authenticity, quality ownership and source confirmation. In the past 10 years, data-hiding technique has been very popular in area of research and watermarking is being the most technique in this area for scholars.

1.2. PREVIOUS RESEARCH WORK ON WATERMARKING

Successive generations of researchers have addressed watermarking techniques and its different aspects.

D. Kahaner, C. Moler and S. Nash, in 1989 proposed numerical methods and software for watermarking techniques which basically gives the computational measures for watermarking methods[1].

Chang Tsun Li et. al. in 1993, describes fragile watermarking scheme for image authentication. In which an efficient fragile watermarking scheme intended for image authentication and integrity verification is proposed. To watermark the underlying image, the gray scale of each pixel is adjusted by an imperceptible quantity according to the consistency between a key dependent binary watermark bit and the parity of a bit stream converted from the gray scales of a secret neighborhood of the pixel. To counter "collage" and "look-up table inferring" attacks, the scanning/watermarking order of the pixels follows a zig-zag path and the secret neighborhood of a pixel is formed by picking previously watermarked pixels before the current pixel on the scanning path[2].

Cox, J. Kilian, T. Leighton, and T. Shamoon in 1997 had proposed technique for secure spread spectrum watermarking for multimedia in which CDMA spread spectrum watermarking is discussed in brief with security issues[3].

Memon, N. and Wong, P., in 1998 gave paper about Protecting Digital Media Content which defines the necessity of protection and security in digital media and also suggested methods for protection of media [4].

Chiou Ting et. al in 1999 shows the survival of watermark after lossy attacks. In experiment, an image authentication technique by embedding digital “watermarks” into images was proposed. Watermarking is a technique for labeling digital pictures by hiding secret information into the images. Sophisticated watermark embedding is a potential method to discourage unauthorized copying or attest the origin of the images. Embed the watermarks with visually recognizable patterns into the images by selectively modifying he middle-frequency parts of the image. Several variations of the proposed method were addressed. The experimental results shown that the proposed technique successfully survives image processing operations, image cropping, and the Joint Photographic Experts Group (JPEG) lossy compression [5].

G. Voyatzis and I. Pitas,in 1999 proposed The use of watermarks in the protection of digital multimedia products which details that digital media can be secured with the help of watermark and the implementation method [6].

G. C. Langelaar, I. Setywan and R. L. Lagendijk, in 2000 gave method for Watermarking digital image and video data, which specifies the size constraints and the different strategies for still and video image [7].

J. Hernandez, M. Amado and F. Perez-Gonzalez,in 2000 proposed DCT domain watermarking techniques for still images in which Detector performance is analyzed and a new structure is proposed for the same [8].

Katzenbeisser S. and Petitcolas F.A.P., in 2000 proposed Information Hiding Techniques for Steganography and Digital Watermarking where the common factors about two methods are discussed and shown that advancement in first results in the second method [9].

Ohbuchi R. et. al in 2002, discussed robust watermarking for digital vector maps. Digital maps are used, for example, in car navigation systems and Web-based map services. As digital data, digital maps are easy to update, duplicate, and distribute. At the same time, illegal duplication and distribution or forgery of the maps is also easy. This research proposes a digital watermarking algorithm for vector digital maps as a method to counter such abuses of the maps. A watermark bit is embedded by displacing an average of coordinates of a set of vertices that lies in a rectangular area created on a map by adaptively subdividing the map. The watermark is resistant against additive random noise, similarity transformation, and vertex insertion/removal, and, to some extent, cropping [10].

R. Liu and T. Tan, in 2002 gave a SVD-Based watermarking scheme for protecting rightful ownership which gives the definition of Digital Rights Management and proposes the scheme for protection [11].

R. Mehul and R. Priti, in 2003 proposed Discrete Wavelet Transform based multiple watermarking schemes which show the DWT algorithm can be implemented in different ways to the watermark [12].

E. Ganic and A. M. Eskicioglu, in 2004 proposed Secure DWT-SVD Domain Image Watermarking in which data is embedded in all frequencies removing the need of only main frequency components and also making the system less complex [13].

Ko Ming et. al in 2004 proposed a novel public watermarking system based on advanced encryption system. Until then many digital watermarking techniques have been proposed to resolve the issues of copyright protection. However, almost proposed watermarking methods keep the watermarking algorithm private to ensure the embedded watermark secret. If the watermarking technique needs to be widespread applied to realistic multimedia environment, the algorithm used by watermarking techniques should be public. In this work, a novel watermarking scheme, which can be public, is presented. The proposed watermarking technique is developed based on the following criterions: first the watermarking algorithm is open; and second the embedded watermark can be extracted and embedded by the people who own the secret key. The watermarking scheme employs the advance encryption standard (AES) and the Reed-Solomon code, to make the watermarking algorithm public. Simulation shows that the proposed algorithm can be very robust to resolve the ownership of the digital image [14].

Fan Jhang et.al. in 2004, did research on watermarking capacity. The work shows image-watermarking capacity is an evaluation of how much information can be hidden in a digital image. Watermarking capacity research studies how to transmit more watermark information. In watermarking schemes, the image is considered as a communication channel to transmit messages. Watermark power should be constrained according to the content of the image. Analyses the shortcomings of some previous watermarking capacity methods and present a watermarking capacity method using the noise visibility function, and discuss the watermarking capacity of blind watermarking and non-blind watermarking [15].

Celik M.U. et.al. in 2006 presented a novel framework for lossless (invertible) authentication watermarking, which enables zero-distortion reconstruction of the un-watermarked images upon verification. As opposed to earlier lossless authentication methods that required reconstruction of the original image prior to validation, the new framework allows validation of the watermarked images before recovery of the original image. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. For verified images, integrity of the reconstructed image is ensured by the uniqueness of the reconstruction procedure. The framework also enables public-key authentication without granting access to the perfect original and allows for efficient tamper localization. Effectiveness of the framework is demonstrated by implementing the framework using hierarchical image authentication along with lossless generalized-least significant bit data embedding [16].

Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, in 2006 proposed concept of Digital Image Watermarking using balanced multiwavelets which includes the wavelets decomposition method for watermarking of images [17].

Xiang-Yang Wang and Hong Zhao, in 2006 proposed A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT in which audio watermarking is done with DCT as well as DWT method to improve the performance of watermark [18].

Steinebach M.i et.al. in 2007 proposed efficient transaction watermarking, a new challenge for applied algorithms arises: Besides the common requirements of transparency and robustness a very fast embedding strategy is necessary as otherwise users would face unacceptable delays before they can download their marked content. This can be addressed either by designing algorithms of very low complexity or by choosing suitable support mechanisms to speed up watermark embedding. The first approach is still an open challenge as watermarking algorithms of low complexity today fail to provide high robustness and transparency. We therefore provide an introduction to three strategies to support fast watermark embedding: Container watermarking based on pre-calculations which today is already used in industrial applications, client-server watermarking where the content is marked after the transfer to the customer and grid watermarking using the computational power of grid networks [19].

Jiang Bin et.al. in 2008 proposed multi-channel DWT domain image watermarking which is robust to geometric attacks, Firstly, this DWT domain watermarking generates a watermarking template referring to one channel DWT coefficients of the image. Secondly, this watermarking template is embedded into other DWT channel of this image. Because both watermarking template and watermarking image undergo same geometric attack, self-synchronization between the embedded watermarking and watermarking image can be obtained automatically during detecting watermarking. Therefore, a high robust performance of resist geometric attack is gained. Finally, several experimental results are given to show that the proposed watermarking algorithm achieves a high robustness even if an image undergoes some serious geometric distortion attacks [20].

Lintav Lv et.al. in 2010 proposed a semi-fragile watermarking algorithm resisting to RST (Rotation, Scaling, Translation). The algorithm can be used to verify the authenticity and integrity of image content. Firstly, the algorithm generates watermarking information by using the edge of the scaled image, and embeds watermarking information based on human visual system. Before detecting watermarking, the parameters of geometric distortions are estimated and restored by using the original moment information. Finally, users compare the extracted watermarking information with the reconstructed watermarking information of the watermarked image to achieve authentication. The experiment results show that the watermarking algorithm has the immunity to common operation (Compression, Noise, Filtering, RST, and so on). The watermarking algorithm can also achieve accurate authentication and tampering localization to malicious processing (Cropping, Replacing)[21].

Shinfeng D. Lin, Shih-Chieh Shie, J.Y. Guoa,in 2010 proposed method for improving the robustness of DCT-based image watermarking against JPEG compression where compression is taken as attack and is dealt with right strategy [22].

2. CONCLUSION

An image authentication technique by embedding digital “watermarks” into images is proposed. Watermarking is a technique for labeling digital pictures by hiding secret information into the images. Sophisticated watermark embedding is a potential method to discourage unauthorized copying or attest the origin of the images. In these work different techniques of watermarking is compared based on timing and psnr value. Based on above comparison an optimum algorithm is chosen and it is modified to enhance the clarity of watermark. In this approach, Cox algorithm is used for watermarking and clarity is enhanced by modifying the algorithm slightly not making it complex. This work also enhances the imperceptibility and robustness of the watermark. The work can be very significantly implanted in today’s digital media world for authentication purpose by selectively modifying the middle-frequency parts of the image. Several variations of the proposed method are addressed. The experimental results show that the proposed technique successfully survives clarity, authentication and imperceptibility issue and being based on cox algorithm it is not much complex also gives optimum psnr.

This method presents a novel framework for lossless (invertible) authentication watermarking, which enables less distortion reconstruction of the un-watermarked images upon verification. As opposed to earlier lossless authentication methods that required reconstruction of the original image prior to validation, the new framework allows validation of the watermarked images before recovery of the original image. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. For verified images, integrity of the reconstructed image is ensured by the uniqueness of the reconstruction procedure. The framework also enables public(-key) authentication without granting access to the perfect original and allows for efficient tamper localization. Effectiveness of the framework is demonstrated by implementing the framework using hierarchical image authentication along with lossless generalized significant bit data embedding.

3. SCOPE OF FURTHER WORK

The experiment deals with the modification in Cox algorithm in DCT domain and in future the same modification can be applied to any of the other watermarking technique like CDMA watermarking, core watermarking, LSB watermarking, or DWT watermarking so that proper clarity can be achieved in watermarked and recovered images.

This experiment can be extended further by using more numbers of PN sequences and the result can be compared. Using more PN sequences will give the image more authenticity but on the other hand, it can increase the complexity and time of watermarking. For highly secured data transmission that experiment would work perfectly with the transmitter and receiver having private key encryption.

The standard 2-band wavelet transforms result in a logarithmic frequency resolution, thereby suitable for analysis of signals with a justified bandwidth. The resiliency, data embedding rate, computational cost, etc all these have to be examined against volumetric distortions in order to get a benchmark algorithm. Therefore, further work is directed towards the testing of resiliency of data embedding process in wavelet domain.

4. REFERENCES

[1] D. Kahaner, C. Moler and S. Nash, Numerical Methods and Software at New Jersey: Prentice-Hall, Inc, 1989.

[2] Chang-Tsun Li "Oblivious fragile watermarking scheme for image authentication" Acoustics, Speech, and Signal Processing, 1993. In ICASSP-93, IEEE International Conference on 27-30 April on pages IV – VI, 1993.

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

[4] Memon, N. and Wong, P., "Protecting Digital Media Content," In: Communications of ACM, Vol. 41, No. 7, pp. 35-43, July 1998.

[5] Chiou-Ting Hsu Ja-Ling Wu , "Hidden digital watermarks in images", Image Processing, IEEE Transactions , issue 1, January on pages 58-68, 1999.

[6] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, Vol. 87, No. 7, pp 1197-1207, July 1999.

[7] G. C. Langelaar, I. Setywan, and R. L. Lagendijk, "Watermarking digital image and video data," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 20-46, Sep. 2000.

[8] J. Hernandez, M. Amado and F. Perez-Gonzalez, "DCT domain watermarking techniques for still images: Detector performance analysis and a new structure", IEEE Trans. Im. Process, Vol: 9, 2000.

[9] Katzenbeisser S. and Petitcolas F. A. P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, UK, 2000.

[10] Ohbuchi, R.; Ueda, H."Robust watermarking of vector digital aps","Multimedia and Expo, In ICME'02. In Proceedings 2002 IEEE International Conference ",on pages 577-580, 2002.

[11] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transactions on Multimedia, 4(1), pp121-128, March 2002.

[12] R. Mehul and R. Priti, "Discrete Wavelet Transform Based MultipleWatermarking Scheme," Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[13] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg,Germany, September 20-21, 2004.

[14] Ko-Ming Chan Long-Wen Chang "Advanced Information Networking and Applications, AINA 18th International Conference ", pages 48-52 vol 1,2004.

[15] Fan Zhang Hongbin Zhang "Communications, Circuits and Systems, ICCCAS 2004. 2004 International Conference" , 27-29 June , pages 796-799 Vol2,2004.

[16] Celik, M.U.; Sharma, G. " Image Processing, IEEE Transactions "April 2006 ,Issue 4 pages 1042-1049,2006.

[17] Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, "Digital Image Watermarking Using Balanced Multiwavelets", IEEE Transactions On Signal Processing, Vol. 54, No. 4, 2006.

[18] Xiang-Yang Wang and Hong Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions On Signal Processing, Vol. 54, No. 12, December 2006.

[19] Steinebach, M. Hauer," Automated Production of Cross Media Content for Multi-Channel Distribution, 2007. AXMEDIS'07. Third International Conference ", 28-30 Nov, pages 65-71,2007.

[20] Jiang-Bin Zheng Sha Feng, "Machine Learning and Cybernetics, International Conference " on 12-15 July ,vol2 pages 1046-1051,2008.

[21] Lintao Lv Liang Hao Hui Lv,"Networks Security Wireless Communications and Trusted Computing (NSWCTC), Second International Conference" on 24-25 April, vol2 on pages 361-364, 2010.

[22] Shinfeng D. Lin, Shih-Chieh Shie, J.Y. Guoa, "Improving the robustness of DCT-based image watermarking against JPEG compression", Computer Standards & Interfaces, Vol: 32, No: 1-2, pp: 54-60, 2010.