International Journal of Computer Network and Security(IJCNS)
Vol 7. No.1 2015 Pp. 9-13
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

A SURVEY ON DIGITAL VIDEO WATERMARKING AND ITS DISCRETE WAVELET TRANSFORM APPROACH

G.SHOBA[1]
Senior Assistant Professor,
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry, India

G.JEYALAKSHMY[2] **M.SHANTHINI**[3] **D.SUGANYA**[4]
M.Tech – Final Year
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry, India
Jeyalakshmy.gopal@gmail.com[2] shanthini.flower@gmail.com[3]
suganyamtechcse@gmail.com[4]

Abstract

Very few authenticating of watermarking schemes have been produced for defining the copyrights of digital video. The process of Digital watermark embeds the data called watermark in digital media like image, video, audio file etc. so that it can be claimed for rights. The paper represents the complete software implementation of 3-Level DWT algorithms and a Secret key is used to have more secure data. The same secret key is used to given the watermark image during embedding process and while extracting the watermark image. To check effectiveness of the watermark video MSE and PSNR are used.

Index: *Watermark, DWT, MSE, PSNR*

1. INTRODUCTION

In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital Watermarking, which is used for authenticating the digital images. The objective is not to protect the Contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, It can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values. There are many spatial and frequency domain techniques available for authentication of watermarking. Watermarking techniques are judged on the basis of their performance on a small set of properties. These properties include robustness, transparency, watermarking capacity, blind detection and security. Watermarking schemes are developed according to the requirements of the application and all applications do not require each of these properties in their entirety i.e. watermarking requirements are application dependent and some most desirable properties for these applications are conflicting in nature. A huge trade-off among them is often involved. Digital signature is also an authentication scheme that is used for verifying the integrity and authenticity of the image content. Digital data are distributed across high-speed networks like the Internet and World Wide Web. This data is easily accessible for sharing. Due to this access possibility of tempering data and republishing it as own is increased. This leads the motivation of techniques providing security to this multimedia content. Digital watermarking is the technique used for this purpose. Various techniques of watermarking are used to insert data about ownership of contents, which help to keep the integrity of data. A watermark is information about origin, ownership, copy control etc. This information is embedded in multimedia content with taking care imperceptibly and robustness. The watermark is embedded and extracted as per requirement. Video watermarking is different from image watermarking, because additional data are available here that allows information to be more redundantly and reliably embedded. Digital video is a sequence or collection of consecutive still images. The amount of information that can be embedded in the video sequence is called payload. In reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of the inherently repeated sequence of data between frames.

1.1 INTRODUCTION TO IMAGE WATER MARKING

Image Watermarking is the technique of embedding owner copyright identification into the host image. The term watermarking was first coined in Bologna, Italy in 1282 in paper mills as paper mark of company. It became common in 20th century. Then watermarks found their place in postage stamp and currency notes. Digital image watermarking is derived from Steganography, a process in which digital content is hidden from the remaining content of message for secure transmission of Digital data. The main goal of steganography is to hide a message ‘m’ in some audio or video (cover) data ‘d’, to obtain new data d', practically indistinguishable from ‘d’, by people, in such a way that an eavesdropper cannot Presence of m in d′. The main goal of watermarking is to hide a message ‘m’ in some audio or video (cover) data ‘d’, to obtain new data d', practically indistinguishable from ‘d’, by people, in such a way that an eavesdropper cannot remove or replace ‘m’ in d'.

2. CLASSIFICATION OF WATER MARKING TECHNIQUES

Video Water marking

Digital watermarking for still images has been extensively studied. Today however, growing popularity of video based applications such as Internet multimedia, wireless videos, personal video recorders, video-on-demand, set-top box, videophone and videoconferencing has increased the demand for a secure distribution of videos. Apparently any image watermarking technique can be extended to watermarking videos, but in reality video watermarking techniques need to meet other challenges than that in image watermarking schemes.

A. Based on Characteristics/robustness

Robust: Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark.

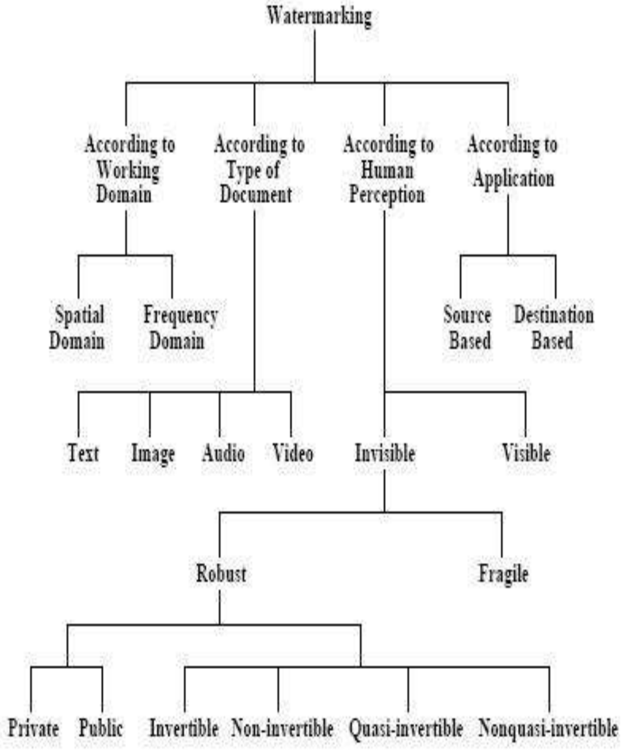

Fig.1: Different Types of Video Watermarking

Fragile: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

Semi fragile: Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression.

B. Based on perceptivity:

Visible watermark: The watermark that is visible in the digital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture.

Invisible watermark: There is technology available which can insert information into an image which cannot be seen, but can be interrogated with the right software. We can‘t prevent the theft of our images this way, but we can prove that the image that was stolen was ours, which is almost as good.

C. Based on domain:

Spatial domain: This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels. Some of its algorithms are LSB, SSM Modulation based technique.

Frequency domain: This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as DCT, DWT, and DFT.

D. Based on detection process:

Visual watermarking: It needs the original data in the testing course, it has stronger robustness, but its application is limited.

Semi blind watermarking: It does not require an original media for detection.

Blind watermarking: It does not need original data, which has wide application field, but requires a higher watermark technology.

3. APPLICATIONS OF DIGITAL WATER MARKING

Copyright Protection: This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

Authentication: Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

Broadcast Monitoring: As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

3 LEVELS DWT

Discrete wavelet transform (DWT) is a mathematical tool for decomposing an image. It is multi-resolution briefing of an image. The decoding can be processed sequentially from a low resolution to the higher resolution. The DWT decomposes the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part splits again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges and range of high frequency. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is an input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes theLL1 band into the four sub bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands: LL3, LH3, HL3, and HH3. In a video, sometimes different video frames are almost identical. A continuous identical video frames is called a video shot. In order to increase the performance of watermark embedding process the proposed system will separate the video into video shots. Each video shot has one or more video frames that are almost identical. In order to determine whether two video frames are identical we compare the two image pixels.

In this paper video watermarking with 3-level DWT is proposed which is perceptually invisible. Perceptually invisible means that the watermark is embedded in video in such a way that the modification to the pixels values is not noticed. In order to solve the copyright protection problem and deceitful alteration by hackers of videos, several watermarking schemes have been widely used. Very few authenticating of watermarking schemes have been produced for defining the copyrights of digital video. The process of Digital watermark embeds the data called watermark in digital media like image, video, audio file etc. so that it can be claimed for rights. The paper represents the complete software implementation of 3-Level DWT algorithms and to have more secured data a secret key is used.

4. CONCLUSION

In this paper video watermarking with 3-level DWT is proposed which is perceptually invisible. Perceptually invisible means that the watermark is embedded in video in such a way that the modification to the pixels values is not noticed. This proposed work by using videos and logo images and shown how watermark is detected and watermarks not detected. Also the use of secret key is explained in brief. To have more security on videos this proposed method is conveniently explained. The MSE should be as low as possible to have less error and the PSNR should be as high as possible to have better quality of reconstructed video.

REFERENCES

[1] Z. Erkin, A. Piva, S. Katzenbeisser, et al., “Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing,” EURASIP Journal on Information Security 2007.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[3] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[4] X. Zhang, G. Feng, Y. Rend and Z. Qian, “Scalable Coding of Encrypted Images,” IEEE Trans. Inform. Forensics Security, vol. 21, no. 6, pp.3108-3114, June 2012.

[5] M. Deng, T. Bianchi, A. Piva, and B. Preneel, “An efficient buyer-seller watermarking protocol based on composite signal representation,” in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[7] W. Puech, M. Chaumont and O. Strauss, “A reversible data hiding method for encrypted images,” Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 68191E, Feb. 26, 2008, doi:10.1117/12.766754.

[8] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Letts. vol. 18, no. 4, pp. 255–258, Apr. 2011.

[9] W. Hong, T. Chen, and H. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Letts. vol. 19, no. 4, pp. 199–202, Apr. 2012.

[10] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[11] K. Ma, W. Zhang, et al. “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, 553-562, 2013.

[12] Z. Qian, X. Han and X. Zhang, “Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2012.