DWT and IDWT Using Secret Key and Watermarking with in Video Compression

G.SHOBA1
Senior Assistant Professor,
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry, India
mailtoshoba@gmail.com

G.JEYALAKSHMY2
M.Tech – Final Year
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry, India
Jeyalakshmy.gopal@gmail.com

Abstract- In this paper, Authenticating watermarking is nothing but inserting a hidden object in order to detect deceitful alteration by hackers. The object may be in terms of a secret key or password etc. There are quite few numbers of authentication methods are available for videos. Resent developers in digital video and internet technology helps the common user to easily produce illegal copies of videos. 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 secure data a secret key is used. The secret key is given to watermark image during embedding process and while extracting the watermark image the same secret key is used. To check effectiveness of the watermark video MSE and PSNR parameters are used.

INTRODUCTION

With the rapid development of Internet technology, such media data as images, audios or videos are used more and more widely in human's daily life. This makes media data not only easy to be transmitted, but also easy to be copied and spread out. Thus, the legal issue rises that some media data should be protected against unauthorized users or operations. To protect media data, two means have been proposed and high-lighted since the past decade, i.e., media encryption and media watermarking. The MPEG-2 video coding standard, which was developed about ten years ago primarily as an extension of prior MPEG-1 video capability with support of interlaced video coding, was an enabling technology for digital television systems worldwide. It is widely used for the trans-mission of standard definition (SD) and high definition (HD) TV signals over satellite, cable, and terrestrial emission and the storage of high-quality SD video signals onto DVDs. However, an increasing number of services and growing popularity of high definition TV are creating greater needs for higher coding efficiency. Moreover, other transmission media such as Cable Modem, xDSL, or UMTS offer much lower data rates than broadcast channels, and enhanced coding efficiency can enable the transmission of more video channels or higher quality video representations within existing digital transmission capacities. The the Video Coding Experts Group(VCEG) ITU-T SG16 Q.6 issued a call for proposals on a project called H.26L, with the target to double the coding efficiency (which means halving the bit rate necessary for a given level of fidelity) in comparison to any other existing video coding standards for a broad variety of applications. Media encryption encrypts media data into unintel ligible ones with ciphers, which protects media content's confidentiality. Taking video encryption for example, the encrypted videos are often difficult to be understood. Different from text/binary data encryption, video encryption often re-quires the scheme be time efficient and format complaint, in order to meet real time applications. It is not practical to encrypt video data completely with traditional ciphers such as data encryption standard (DES) or advanced encryption standard (AES), because of high computational cost. Information processing in the encrypted domain has attracted considerable research interests in recent years. In many applications such as cloud computing and delegated calculation, the content owner needs to transmit data to a remote server for further processing. In some cases, the content owner may not trust the service supplier, and needs to encrypt the data before uploading. Thus, the service provider must be able to do the processing in the encrypted domain. Some works have been done for data processing in an encrypted domain, for example, compressing encrypted images, adding a watermark into the encrypted image, and reversibly hiding data into the encrypted image.

RELATED WORK

Discrete Wavelet Transform

The use of Wavelet transform will mainly address the capacity and robustness of the Information Hiding system features. The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients that are generated by taking half of the difference of the same two pixels.

The four bands obtained are LL, LH, HL, and HH. The LL band is called as approximation band, which consists of low frequency wavelet coefficients, and contains significant part of the spatial domain image. The other bands are called as detail bands which consist of high frequency coefficients and contain the edge details of the spatial domain image. Integer wavelet transform can be obtained through lifting scheme.

Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information.

Transform-domain techniques, on the other hand, alter spatial pixel values of the host video according to a pre-determined transform. Commonly used transforms are the Discrete Cosine Transform (DCT), the Fast Fourier transform (FFT), the Discrete Wavelet Transform (DWT), and the Singular Value Decomposition (SVD). Transform-domain watermarking techniques proved to be more robust and imperceptible compared to spatial domain techniques since disperse the watermark in the special domain of video frame, making it very difficult to remove the embedded watermark. The watermarking may be visible or invisible. In this paper proposed an invisible watermarking technique based on 3 levels DWT. DWT is more computationally efficient than other transform methods like DFT and DCT. Due to its excellent spatio frequency localization properties, the DWT is very suitable to identify areas in the host video frame where a watermark can be embedded imperceptibly. It is known that even after the decomposition of the video frame using the wavelet transformation there exist some amount of correlation between the wavelet coefficients.

EXISTING SYSTEM

RDH (Reversible Data Hiding) methods for encrypted images can be classified into two categories: "vacating room after encryption (VRAE)" and "vacating room before encryption (VRBE)". In VRAE the original image is encrypted directly by the sender, and the data-hider embeds the additional bits by modifying some bits of the encrypted data. On the receiver side, data extraction and image recovery are realized by analyzing the local standard deviation during decryption of the marked encrypted image. This method requires that image decryption and data extraction operations must be done jointly. In other words, extraction and decryption are inseparable. In the VRBE, the original images are processed by the owner before encryption to create spare space for data embedding, and the secret data are embedded into specified positions by the data-hider. It requires that the sender must perform an extra RDH before image encryption. This may be impractical, in case the sender has no idea of the forthcoming data hiding by the data-hider, or receiver has no computational capability of the traditional RDH. On the other hand, in case the sender can reserve room for embedding by reversibly hiding redundant bits into the original plain image, all embedding tasks can also be done on the sender side and then the data-hider becomes redundant. This estimation is not accurate enough. The reversible data hiding (RDH) in encrypted images using distributed source coding (DSC). In case the receiver has the encryption key only, receiver can recover the original image approximately with high quality using an image estimation algorithm. The proposed estimation algorithm can also be used to find empirical error probability of the virtual channel. With a database containing numerous natural images, we perform the estimation algorithm to generated estimated images.

DISADVANTAGES

- Process is not accurate enough
- Information losses
- Extraction and decryption are inseparable

PROPOSED SYSTEM

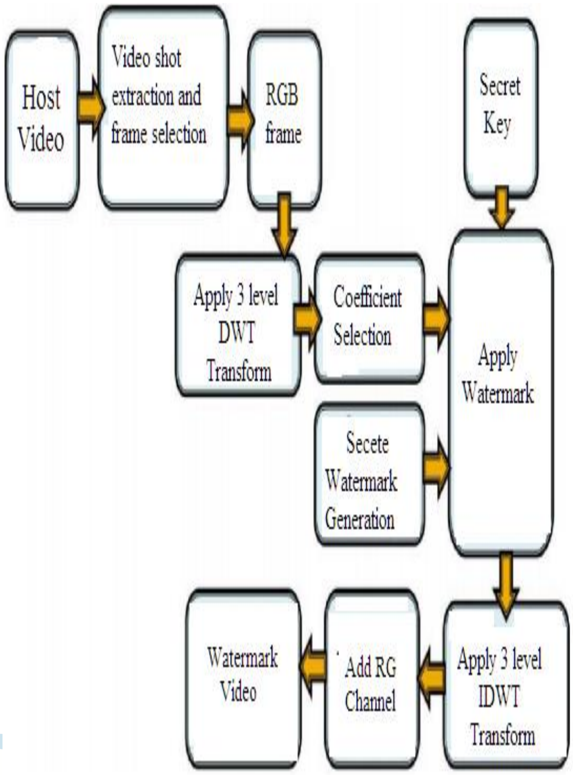
In this paper video watermarking with 3-level DWT is proposed which is perceptually invisible. Perceptually invisible means that the watermark is embedded in video in such a way that the modification to the pixels values is not noticed. In order to solve the copyright protection problem and deceitful 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 secure data a secret key is used.

ADVANTAGES

- High security
- Good for secure media transmission or distribution
- Increases the operation efficiency

SYSTEM ARCHITECTURE

Watermark Embedding Process A continuous 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. According to video standard, the intensity for a RGB frame can be calculated as, pixel. Generally, the human visual system is least sensitive to the range of high frequency. Among three channels of the RGB image, the blue channel has characteristic of the highest frequency range. So, for the high performance the blue channel is transformed into DWT and the watermark is embedded from HL3 sub-band of the blue channel of the host video frame. If the HL3 sub-band is fill-up then the remaining watermark signal is embedded in LH3 sub-band.


Host Video
Video shot extraction and frame selection
RGB frame
Secret Key
Apply 3 level DWT Transform
Coefficient Selection
Apply Watermark
Secete Watermark Generation
Watermark Video
Add RG Channel
Apply 3 level IDWT Transform

Again, if the LH3 sub-band is over then HH3. If HH3 is over then the next upper level is used that is HL2, LH2, HH2 is used. In this way all the watermark is embedded into the video frame.

The proposed embedding process, after separating the video into video shots the system will apply 3L-DWT on the blue channel of RGB frame. In the 3L-DWT coefficients, embed pre processed watermark image from the HL3 to HH1 sub-band consecutively and then it is transformed into 3-level inverse DWT form. At this stage, for RGB video frame we get the watermarked blue channel which is then combined to other two channels to obtain the watermarked video frame. The secret key is added before embedding process. A dialog will open “enter secret key”. After entering secret key pop up message shows secret key inserted successfully.

RESULTS AND EVALUATION

The proposed technique has been Selecting an image and applying 3-Level DWT. selecting an image to be watermark in video. The watermark image is hide in that input image and the embedding process is carried out after this the 3 level inverse DWT is applied and again converting it in to image. Video is reconstructed and it seen that there is not much difference between input image and the reconstructed. The performance of reconstructed video is measured by two factors namely: Mean Square Error (MSE) and Peak Signal to Noise Ratio (PNSR).

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, 2008.

[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. Ren 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. Lett., 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. Lett., 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,” 3rd International Conference on Multimedia Technology (ICMT 2013), pp. 869-876, Guangzhou, China, 2013.

[13] W. Zhang, K. Ma and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Processing, vol. 94, pp. 118–127, 2014.

[14] T. Kalker and F. M. Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[15] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[16] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[17] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[18] D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.