Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.796 – 801

RESEARCH ARTICLE

A DWT and DCT Based Hybrid Approach for Video Watermarking

Arti[1], Neeraj Dahiya[2]

M.Tech Student CSE Dept., South Point Institute of Technology and Management, Sonipat, Haryana
malikarti66@gmail.com

Assistant Professor CSE Dept., South Point Institute of Technology and Management, Sonipat, Haryana
dhynrj@gmail.com

Abstract— Watermarking is about to authenticate the digital contents by embedding the copyright signature in information object itself. In this work, the watermarking is defined for video objects. The work is defined as a layered approach in which the video is splited in video frames to perform watermarking. At the earlier stage, the compression on the information object is applied to increase the capacity of cover object. The compression is here performed using DWT approach. In second layer, the selection of effective frames is obtained to increase the security level. The duplicate frame removal is performed at this stage using similarity analysis approach. At the final stage, DCT is applied to hide the information object in selected frames. The work has increased the security and reliability for watermarking process.

Keywords- Audio Watermarking, DWT, DCT, Noisy, Compression

I. INTRODUCTION

Watermarking is about to perform the information hiding in different digital objects to prove the authentication to the individuals. This kind of system improves the integrity over the signal so that the information can be placed in public domain. This watermarking concept reserves the information object based on this authentication object. In this work, the watermarking is defined for video contents. The exclusive videos captured by an individual are required to reserve such as the movies etc. It is required to reserve these movies to the particular banner. To perform this organization logo or the authentication mark is embedded to the video itself. To protect such kind of video contents and to provide the copy protection, a Copy Protection Technical Working Group (CPTWG), Motion Picture Association of America, the Consumer Electronics Manufacturers Association, and members of the computer industry, examines the digital Content protection in the form of Video watermarking. These organizations provide the copyright protection for DVD. The video watermarking provides the information protection under the authentication level. It provides the information whether the object is copied or node as well as number of times copy performed. This authentication mechanism is having the advantage in terms of cost effective approach. It provides the security and reliability in terms of lesser chances of watermark distortion. This kind of watermarking approach integrated defined with different decoders such as MPEG decoder. Watermarking ensures the multimedia content is available in the DVD. To improve the information security, the watermarking approaches also combined with other authentication features such as cryptography. This is actually the encoding mechanism in which the watermark is embedded in encoded form. This kind of approach is applicable only for invisible watermarking. The security of this approach can also be enhanced by performing the key oriented watermarking or cryptography. The type of key used also improves the reliability and integrity of watermark system.

To improve the strength of watermarking, instead of embedding single watermark, two or more watermark objects can be used. These watermarks can be performed on different frames and by using different approaches. The ticket counter based watermarking approach is also used in may video marking system. The advantage of this approach is to update the watermark with each relative operation. This approach provides the dynamic watermark generation each time the video contents are copied to some other media from the DVD. Video watermarking also support the concept of scene based watermarking. This kind of approach provides the frame separation from the video and identifies the effective frames on which the watermarking will be performed. These frames can be static or dynamic. The wavelet based decomposition approach can be applied to perform such kind of watermarking. To improve the capacity of the watermarking, the compression technique can also be integrated at some layer in the watermarking process. This kind of compression can be performed at low level to define the length decoding process so that the watermark complexity will be reduced and the system reliability will be improved.

A) Video Watermarking Requirement

Video watermarking is opted to secure the digital video content from unauthorized access. The basic requirement of such watermarking systems is given in this section. The first associated requirement is the recognition of the video format. The video watermarking is generally dependent on the video format. If the video is in compressed domain, the watermarking will not be much effective. The video type defines the robustness of the watermarking system. This kind of approach also requires the fast information processing. As the size of video can be large, but even though the efficiency of watermarking process is the basic requirement. In case of video watermarking, sometimes the hidden object is not available in original form. In such case blind watermarking is required to perform the information hiding and retrieval.

B) File Format

There are number of available formats for video information processing. These video formats are different in terms of quality, frame rate and the size of video. The low quality videos are generally the compressed video. Watermarking on high quality audio is generally preferred. One of such high quality format is the AVI format used in this research work. This form of video is not compressed form and provides the effective watermarking. Some other formats include the mpg, mov etc.

In this research work, an effective layered approach is defined for video watermarking. This approach is a scheme based approach in which DWT and DCT are combined to perform the watermarking. DWT is here performed to compress the hidden object and to improve the watermark capacity. DCT is actually defined to perform watermarking on individual frame. In this section, the video watermarking is defined along with relative issues. In section II, the work defined by the earlier researchers is discussed. In section III, the proposed research work is defined. In section IV, the results obtained from the work are discussed. In section V, the conclusion obtained from the work is presented.

II. LITERATURE REVIEW

In this section, the work defined by the earlier researchers on watermarking approaches for different media types is discussed. Bender et al. [1] has defined a data hiding scheme and evaluation with traditional watermarking schemes. Author defined the evaluation process for three different application areas called copyright protection, augmentation data embedding and tampers proofing. Author discussed the different properties of watermarking process along with the quality and quantity analysis for the hidden object. Author performs the invariance analysis over the data under different condition so that the distortion over the information object will be recognized. Author defined the lossy compression along with degree specification and interception to the third party will be done. Currie et al. [2] defined an effective data hiding approach along with compression approach. Author used the JPEG compression approach to reduce the information size and to avoid the visual distortion. Author also introduces the error analysis against the bitmap data. Author defined the error analysis under the compression so that the information encoding to the pixel form will be done effectively. Author provides the information hiding along with accurate information extraction. Handel et al. [3] defined a development tool for the extraction of hidden challenge so that the effective communication over the network will be performed. Author defined the cryptography approach along with watermarking to improve the information security and provide the network model along with object hiding and detection in summarized form. Author discussed various methods of hiding objects in summarized form. Anderson et al. [4] presented an analysis to the data hiding concept under the contrast analysis so that the effective cryptography will be obtained. Author analyzed the work under different kind of attacks so that the information hiding will be performed effectively. Author improved the consideration of information hiding under different signal process methods such as amplify the covertness and also provided the key based information storage over the system.

Johnson et al. [5] presented a characteristic analysis based data hiding concept so that the information message will be stored. Author also defined the approaches to recover the information messages without proper algorithmic implementation. Lee et al. [6] defined an approach for the data hiding model to improve the image fidelity. Author used the LSB approach to perform information embedding over the cover object. Author [7] defined the pixel wise and bit wise approach to improve the information object security and authenticity. Author provided the techniques to improve the information security so that information contents will be hide over the image. Dunbar et al. [8] provided an overview to the data hiding schemes and provides the information communication in open environment. Author provided the tool and resource based analysis to analyze the system integrity and security. Ahsan et al. [9] defined an improved steganographyic system for wireless network. Author provided the secure telecommunication over the network integrated with cryptographic system. Author[10] defined the model to provide the effective bandwidth allocation so that the information will be stored in corrupt frames. Author provide the analysis under different approaches to improve the system integrity and the reliability.

Wang et al. [11] presented the battle between steganography and steganalysis. The two sides of the battle are the attempt to transmit secret messages under cover of innocuous multimedia signals and the effort to detect or prevent such hidden communication. Several Steganographic techniques and steganography detection methods were studied and compared. Vidyasagar M. Potdar et al. [12] presented a detailed survey of existing and newly proposed steganographic and watermarking techniques. The techniques were classified based on different domains in which data is embedded.

III. PROPOSED APPROACH

Video watermarking is the authentication approach to claim the rights over some digital video contents over the web. In this work, an intelligent layered approach is suggested to perform the video watermarking. Instead of hiding the watermark image over all video frames in this work a unique frame selection scheme is suggested to hide watermark only behind the unique frames. Moreover, instead of hiding the watermark in traditional way, at first the compression will be performed using DWT approach and later on the DCT will be used to perform the watermarking.

The watermarking over the video frames will be performed sequentially and only performed on the unique frames.. The result analysis will be performed in terms of extraction of the watermarked image from the video under analytical parameters such as MSE, PSNR etc. The presented work includes the following major steps.

In the watermarking approaches the complete watermarked image is embedded in each frame or the random frames of the video but in this work an intelligent approach is defined to perform the watermarking by performing the compression at the earlier stage. The first layer of work includes the compression of input watermark image. For this kind of sub image compression, a wavelet based approach is suggested. The approach will be taken to reduce the watermark image size and the compression will be kept in limit so that no much data loss will be performed.

Once the compression is done, in next stage, the DCT will be implemented to perform the watermarking. For this, at first the video splition will be performed to extract the video frames from the video and later on watermarking will be performed over these video images. The presented approach will provide the high degree of authentication as well as the save the data area. In this work, the watermarking will not be performed on all frames of the video, instead of that at first the unique frames will be identified from the video and then the watermarking of compressed image will be performed.

The complete work is divided in three main stages. In first stage, the equational analysis will be performed to identify the unique frame or the images from the video. In second stage the compression will be performed using DWT to increase the capacity of watermark image and at the third stage, DCT will be used to perform the data hiding over the unique frames.

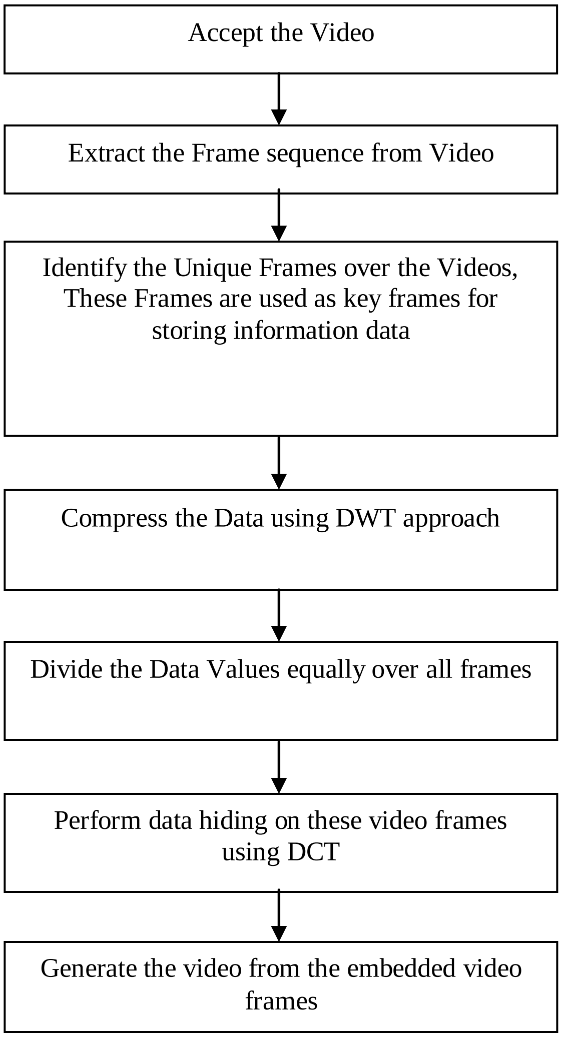

Accept the Video
Extract the Frame sequence from Video
Identify the Unique Frames over the Videos, These Frames are used as key frames for storing information data
Compress the Data using DWT approach
Divide the Data Values equally over all frames
Perform data hiding on these video frames using DCT
Generate the video from the embedded video frames

Figure 1: Flow of Work

The concept defined in this paper is based on DWT and DCT approaches. These two approaches are defined here under

A) DCT

DCT is one the widely used decomposition approach that divided the input signal under frequency level analysis. This approach is based on the cosine transformation of the signal. Once the information data is converted to the signal form, the frequency domain based analysis is performed over it. The concept of DCT approach comes under spatial domain and frequency analysis. In this work DCT is applied to hide the information object in video frames.

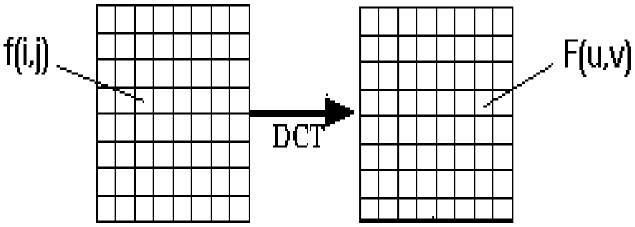


Figure 2 :DCT Encoding

The DCT process stages are given here under

- Identify the effective video frames and apply DCT decomposition over it.
- DCT divides the frames in smaller segments of size nxm.
- Identify the high intensity blocks from the video frames and enable the information storage over it.
- Perform the coefficient analysis over it and to perform the window generation and extraction to perform watermarking.
- Generate the DCT matrix to define the information level.
- Retrieve the matrix contents in specific order to perform the data hiding

B) DWT

DWT is another decomposition approach defined under frequency domain. DWT approach accepts the information object and performs the localized frequency analysis under the frequency specification and localization. DWT divides the information frame in four blocks and perform the coefficient analysis on it. The detailed coefficient analysis is performed for horizontal, vertical and diagonal analysis and approximate coefficient analysis is performed for lower frequency information extraction. In this work DWT is applied to perform the compression.

IV. RESULTS

The presented work is implemented in matlab environment and tested on different audio files. The result analysis is performed on different videos. The avi file type is accepted here to hide the information object in videos. The analysis of the work is done in terms of BER and PSNR values. The analysis results obtained from the work are presented here under.

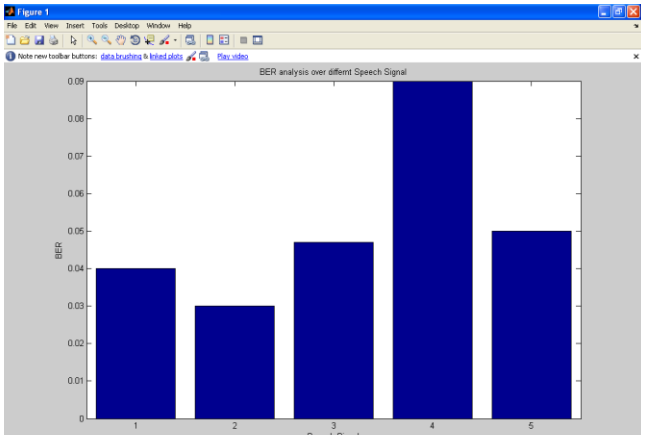
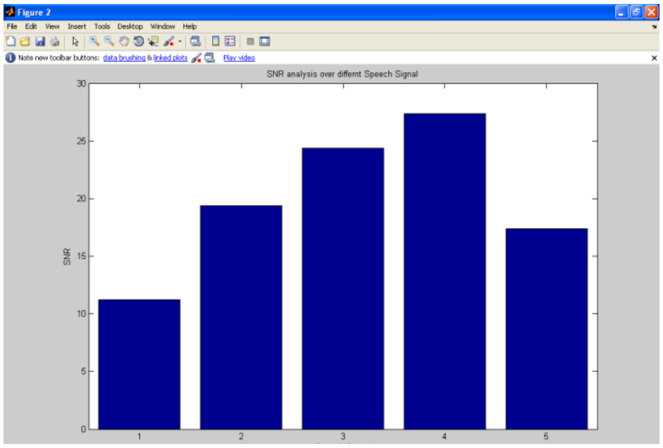


Figure 3 : BER Analysis

Here figure 3 is showing the result analysis for 5 different videos for BER analysis. The figure shows, most the video provided the effective results in terms of BER analysis. Only video 4 is not much effective under this parameter.



Note new toolbar buttons: data brushing & linked plots Play video

Figure 4 :PSNR Analysis

Here figure 4 is showing the result analysis for 5 different videos for PSNR analysis. The figure shows, most the video provided the effective results in terms of PSNR analysis. Only video 4 is not much effective under this parameter.

V. CONCLUSION

In this paper, an effective approach is defined to perform watermarking for videos. The work is defined using a layered approach that combined the DWT and DCT approach for scene based watermarking. The DCT is here applied for information hiding and DWT is performed for the compression. The obtained results show the effective extraction of results from the system.

References

[1] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal,Vol 35, 1996.

[2] Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography”, 19th National Information Systems Security Conference, 1996.

[3] Handel, T. & Sandford, M., “Hiding data in the OSI network model”, Proceedings of the 1st International Workshop on Information Hiding, June 1996.

[4] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998.

[5] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, Proceedings of the 2nd Information Hiding Workshop, April 1998.

[6] Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, Visual Image Signal Processing, 147:03, June 2000.

[7] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001.

[8] Dunbar, B., “Steganographic techniques and their use in an Open-Systems environment”, SANS Institute, January 2002.

[9] Ahsan, K. & Kundur, D., “Practical Data hiding in TCP/IP”, Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[10] Venkatraman, S., Abraham, A. & Paprzycki, M., “Significance of Steganography on Data Security”,Proceedings of the International Conference on Information Technology: Coding and Computing,2004.

[11] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, 47:10, October 2004.

[12] Vidyasagar M. Potdar, Song Han, Elizabeth Chang “A Survey of Digital Image Watermarking Techniques” 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).