e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Review on FPGA Based Digital Watermarking Techniques for Video Authentication

Dilip B.Parmar[1], Mrs.Hina Patel[2],
[1]*PG Student*, *Department of Electronics & Communication, Parul Institute of Technology, Limda,Gujarat,India*
[2]*Asst.Professor*, *Department of Electronics & Communication, Parul Institute of Technology, Limda,Gujarat,India*

Abstract—Digital watermarking is one of the information hiding technology which provides the authentication and copyright protection. The digital videos are easily exchanged through internet and threaten to various malicious attacks so they must be protected based on copyright. This paper present an efficient hardware based concepts of digital Watermarking system which features low power consumption, efficient and low cost implementation, high processing speed, reliability and invisible, semi-fragile watermarking in compressed video streams. Presented system can also features minimum video quality degradation and also can tolerate various potential attacks i.e. cropping, segment removal on video sequences. Proposed concepts can be implemented using VHDL synthesize Into FPGA.

Keywords- Digital Watermarking, Attacks, DCT, DWT, Quality Performance Measure, FPGA

I.INTRODUCTION

Nowadays due to the rapid growth of multimedia processing techniques video data can be distributed easily and fastly. Digital video sequences are very susceptible to manipulation. It is more significant where video is to be used as evidence. In this type of situation video data are more credible so its authentication is needed for its authenticity and security of its content. That is why digital watermarking has been considered as one of the key authentication method. Digital watermarking is the process of inserting information into a multimedia content like audio, text, images or video. By inserting watermark to the multimedia we can verify the ownership of the digital media.[1] Digital watermarking is similar to watermarking technique which allows an individual to add exclusive rights notices or other verification messages to digital media. video authentication's one of the applications of digital watermarking, which is used for authenticating the digital video. A digital watermark is a kind of marker covertly embedded in a noise-tolerant image such as audio or image data. It is typically used to identify ownership of the copyright of such video sequences. There are some various algorithms are used to hide the information into the digital media like least significant bit(LSB) and patchwork algorithm which are spatial domain technique of digital watermarking whereas Discrete cosine transform(DCT) and Discrete wavelet transform(DWT) which are frequency domain techniques of digital watermarking.LSB technique can be implemented easily and take less time but it is less robust compared to both DCT and DWT. Watermarking using DCT and DWT separately have their individual advantages. This proposed method introduce video watermarking using both algorithm DCT and DWT then it is to be implemented on FPGA which features low power consumption, efficient and low cost implementation, high processing speed.

II.CHARACTERISTICS OF DIGITAL WATERMARKING

Digital watermarking have following characteristics.

Robustness: It is the capability of the watermark to resist change after normal image processing operations such as image cropping, transformation, compression etc.

Imperceptibility: This indicates image should preserve its appearance after been watermarked means the watermarked image should appear like same as the original image to the ordinary eye. The observer cannot detect that watermark is embedded in it.

Capacity: Capacity indicates how many information bits can be hide in one document.

III.PROPERTIES AND ATTACKS ON DIGITAL WATER MARKING

Effectiveness: It indicates that the message in a watermarked image will be correctly detected.
Image fidelity: It is the property which says that Watermarking is a process that alters an original image to add a message to it; therefore it certainly affects the image's quality. We want to keep this poverty of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed.
Payload size: It defines the size of the data which is to be inserted into cover image.
Various attacks affecting Digital watermarking:
There is a possibility of various malicious intentional or unintentional attacks that a watermarked matter. A various types of watermarking attacks is follows.
Removal Attack: It removes the watermark data from the watermarked object.
***Geometric attack*:** This attack includes all manipulations that distress the geometry of the image such as flipping, rotation, cropping, etc. should be detectable.
Cryptographic attacks: It is deal with the brilliant of the security.

IV.APPLICATION BASED ON DIGITAL WATERMARKING

Copyright protection: It is used to identify and protect official document ownership.
Digital right management: It can be used for description, identification, trading, protecting, monitoring and tracking of all forms of usages over tangible and intangible assets.
Tamper proofing: It is used for fragile in nature.
Broadcast monitoring: In which application the number of television and radio channels delivering content has notably expanded.
Fingerprinting: Fingerprints are the description of an object that tends to differentiate it from other small object .
Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking.
Image and content authentication: In this application the objective is to detect modification to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences.

V.VIDEO WATERMARKING TECHNIQUES

Spatial domain: Algorithms directly load the raw data into the original image. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing [6].

Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks . LSB is very sensitive to noise and common signal processing and cannot be used in practical applications[6].

Patchwork Algorithm: Patchwork is a data hiding technique developed by Bender et al. and published on IBM Systems Journal, 1996. It is based on a pseudorandom, statistical model[6]. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution.

Frequency domain: Compared to spatial-domain methods, frequency domain methods are more commonly applied. The aim is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain, that is the characteristics of the human visual system (HVS) are better captured by the spectral coefficients[6].

Discrete cosine transforms (DCT): DCT represents data in conditions of frequency space relatively than an amplitude space. It is useful, because that corresponds more to the way humans observe light, so the part are not supposed can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more costly[6].

Discrete wavelet transforms (DWT): Wavelet Transform is a recent technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration.[6] The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal.

VI.DISCRETE COSINE TRANSFORM (DCT)

In Discrete Cosine Transform, an image is broken up into different frequency bands, to get middle frequency bands of an image where watermark can be embedded easily[7].

The following are steps carried out in the encoding procedure of DCT:

1. The image is broken into N*N blocks of pixels.
2. In matrix multiplication the DCT is applied to each block from left to right, top to bottom.
3. Each block's element is compressed through quantization means dividing by some specific value. Qunatization is achieved by dividing each element in transforming image matrix by the corresponding element in quantization matrix.
4. The array of compressed blocks which represent the image is stored in a reduced amount of space. It is carried out using zig-zag sequences.

VII.DISCRETE WAVELET TRANSFORMS (DWT)

The DWT decomposes an input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns[7].

The basic idea in the DWT for a one dimensional signal is the following. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the signal are largely confined to the high frequency part. The low frequency part is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times, which is usually determined by the application at hand.

In the encoding part of DWT while watermarking, we first decompose an image into several bands with a pyramid structure and then add a pseudo-random sequence (Gaussian noise) to the largest coefficients which are not located in the lowest resolution.

VIII.VIDEO WATERMARKING USING COMBINED DWT AND DCT

The watermarking algorithm is presented as follows[5]

- Extract the reference frames from the host color video.
- Choose the key frames amongst the entire set of frames on a random but recurring basis to embed watermark.
- The second level Discrete Wavelet Transform decomposition is carried out on these frames.
- The Discrete Cosine Transform is applied on high frequency coefficients.
- Similarly DCT is also applied on the colour watermark to be embedded.
- Embed this watermark into the selected frames such as HL and LH wavelet bands in second level decomposition. The mid frequency DCT coefficients of the key frames are altered by low frequency DCT coefficients of watermark.
- Combine all these frames i.e. the unmarked as well as the watermarked frames to reconstruct watermarked video.
- The original video and embedded video are compared on the basis of subjective as well as objective criteria.
- The embedded video and embedded key frames are modified using image and video processing to verify the robustness of the algorithm.

Extraction Algorithm:

The reference frames are separated from the watermarked video during extraction procedure. Any one marked frame is selected for retrieval process of embedded watermark. The second level DWT decomposition is applied followed by DCT applied on the high frequency bands. The mid frequency coefficients are selected and used for reconstruction of the watermark [5].

- Extract the reference frames from the embedded color video.
- Choose the marked key frames amongst the entire set of frames as the selection of frame during embedding process is done on a random but recurring basis.
- The second level Discrete Wavelet Transform decomposition is carried out on one of the marked frames.
- The Discrete Cosine Transform is applied on these high frequency coefficients.
- The mid frequency coefficients are taken out to use in reconstruction process.
- The DCT is also applied on the original watermark which was embedded.
- The coefficients separated in step 5 are replaced at the location of the low frequency DCT coefficients. The inverse DCT is applied on these coefficients to reconstruct watermark.
- The original watermark and reconstructed watermark are compared based on subjective as well as objective criteria to check the robustness of the algorithm.

IX.QUALITY PERFORMANCE MEASURES

Mean square error (MSE): It is defined average squared difference between to reference image and distorted image.It is calculated by the formula given below[6].

$$\mathbf{MSE=1/XY\ [\sum_{I=1}^{X}\ \sum_{J=1}^{Y}\ (C(i,j)-e(i,j))^2]}$$

Where,
X and Y are height of the video frame.
C (i, j) is the pixel value of the cover image or frame.
e (i, j) is the pixel value of the embed image of frame.

Peak signal to noise ratio (PSNR): It is used to determine the degradation in the embedded image with respect to the host image [ijeit]. It is calculated by the formula as,

$$\mathbf{PSNR=10log_{10}(L*L/MSE)}$$

Where, L is the peak signal value.

X.FPGA

Field programmable Gate arrays have become the dominant kind of programmable logic device.[12] FPGA can implement too much larger logic function compare with previously programmable device like PAL (Programmable Array Logic) and CPLD (complicated programmable logic device). FPGA could be a very large scale integrated circuit which will be re-programmed. FPGA provides designers with reconfigurable logic that can be reprogrammed as per the user requirement. This ability in FPGA increases flexibility in the event of image processing algorithm on FPGA. The special potential of the FPGA is parallel processing and high computational density as compared to the general purpose microprocessor. This step is combining together with the capacity of FPGA being re-programmable and because this reason FPGA become the dominant form of the programmable logic device which play a useful role for implementation of image processing as well as in video processing algorithms.

XI.CONCLUSIONS

This paper presents digital watermarking technique for video authentication using combination of both algorithm DWT and DCT, which is then can be implemented on FPGA for achieving a certain level of security, high processing speed, minimum video quality degradation and low power consumption.

REFERENCES

[1] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, "Hardware implementation of a digital watermarking system for video authentication',IEEE VOL.23, Feb. 2013.

[2] Prof.R.V.Babar, Mr.Akshay.A.Jadhav, "LSB & DWT Based digital watermarking system for video authentication",IJTRA,Vol.2,May-June 2014.

[3] Yong-Jae Jeong, Wow-Hee Kim, Kwang-Seok Moon, and Jong-Nam Kim, "FPGA based implementation of real time watermarking for high definition video"IEEE, Dec,2009.

[4] Mr.Amit M Joshi, Dr. R.M.Patrikar, Dr.Vivekanand Mishra, "Design of low complexity video watermarking algorithm based on integer DCT" IEEE,2012.

[5] Aditi Agrawal, Ruchika Bhadana,Satishkumar Chavan, "Robust video watermarking scheme
Using DWT and DCT " IJCSIT, Vol.2,2011.

[6] Mohan Durvey, Devshri Satyarthi, " A review paper on digital watermarking" IJETTCS, Vol.3, July-Aug 2014.

[7] Gopika V Mane, G. G. Chiddarwar, "Review paper on video watermarking techniques" IJSRP ,Vol.3, April 2013.

[8] Manpreet kaur, Sonia Jindal, Sunny behal, " A Study of Digital image watermarking" , Proceedings of Volume2, Issue 2, Feb 2012.

[9] G. Dayalin Leena and S. Selva Dhayanithy, "Robust Image Watermarking in Frequency Domain", Proceedings of International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 2 No. 4 Apr. 2013, pp. 582-587

[10] Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang"A Watermarking Technique based on the Frequency Domain", Proceedings of Journal of Multimedia, 2012,Vol. 7, No. 1, pp. 82-89.

[11] Mr.Ashish S.Bhaisare, Prof. A. H. Karode, Prof. S.R.Suralkar, "Significance Research Review on Real Time Digital Video Watermarking Systemfor Video Authentication" Conf. on CEEE 2013.

[12] "Digital image processing" , by Rafael C. Gonzalez, Richard E. Woods, PEARSON.