ISSN 2349-0292
Impact Factor 2.365

Global Journal of Advanced Engineering Technologies and Sciences

CRYPTOGRAPHY IN DIGITAL MULTIMEDIA BASED ON VLSI

Mr.Sachin C. Rathod[*1], Mr.Anilkumar Vishwakarma
[*1]Asst Prof.LokmanyaTilak College of Engineering, Koperkhairane,Navi Mumbai.
Associate Prof. GF's Godavari college of Engineering,Jalgaon.

Abstract

Watermarking in digital cryptography is a technique which allows somebody else to add hidden copyright notices or otherVerification messages to digital audio, video, or image signals and documents. Such a message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. There are different techniques used to perform watermarking. Various comprehensive investigations on the existing watermarking technologies have been accomplished. In the current paper we are going to present the different review of the video watermarking. In this paper we proposed FPGA Implementation for DCT based video watermarking system.

Keywords: MJEPG, FPGA, Video Watermarking, DCT, etc.

Introduction

Video Watermarking offers a wide range of new capabilities to multimedia applications. It allows the indexing of video mail by permitting the insertion of comments in video content as well as the indexing of movies or news items by making available the utilization of markers that can be exploited in search engines. As the number of images and video contents online increases a lot faster than the capabilities of today's search engine, it is important to plan ahead for new ways to allow quick access to multimedia data and watermarking is certainly a promising way to do so.Video watermarking allows us to protect the video mediafrom unauthorized used.

Watermarking is copyright protection. The owner of the original data wants to prove his/her ownership in case the original data is copied, edited and used without permission of the owner. The following are some requirements that a watermark algorithm in part or in full must be held.

Robustness

Robustness means that the watermarking scheme employed should be able to preserve the watermark under various attacks.

Quality of the image

Watermarking should be done in a way such that it doesnot affect the quality of the video or the hidden data after watermarking. The changes in the image should not be noticeable to the naked eye.

Reliability of the watermark

There is always a possibility that the user knows the exact algorithm for detecting and rendering the watermark inactive. The only way to secure the watermark then lies in the selection of the key used for watermarking. Now, even if the user on the other side knows the exact algorithm it should be practically impossible to find the exact key to match with the one during embedding. This counts for the reliability or strength of the watermark.

Universal

Watermark should be universal, i.e. applicable to images as well as audio and video media. In fact, that has been found not to be true; the general concept might be the same in multiple applications but, in watermarking, one size does not fit all . As it might already be obvious for an attentive reader, a lot of difficulties are encountered while trying to define the ideal watermarkingscheme for a particular application. Some particular attention must be paid in order not to downgrade the quality of image.

ISSN 2349-0292
Impact Factor 2.365

Security
One should assume that the method used to encrypt the data is known to the unauthorized party. It means that watermarking security can be interpreted as encryption security leading directly to the principle that it must lie mainly in the choice of the embedded key.

Imperceptibility
The imperceptibility refers to the perceptual similarity between the original and watermarked data. The owner of the original data mostly does not tolerate any kind of degradations in his/her original data.

Literature Survey

Ashish M. Kothari (2012): In this paper, we emphasized on the transform domain method for the digital watermarking of video for embedding invisible watermarks behind the video. It is used for the copyright protection as well as proof of ownership. In this paper we have specifically used the characteristics of 2-DDiscrete wavelet Transform and discrete cosine transform for the watermarking. In this work we first extracted the frames from the video and then used Frequency domain characteristics of the frames for watermarking. We calculated different parameters for the sake of comparison between the two methods.

Yujie Zhang (2012): This paper presents a video watermarking algorithm in detail based on DCT, DWTand neural network technology and digital watermarking was proposed and a professional video copyrightprotection platform was built using the above algorithm. This algorithm effectively enhances therobustness of the video stream. The platform includes video watermark embedding, watermark detection and video piracy tracking and other functions. It doesn't only achieve the prevention beforehand but also the piracy tracking afterwards. The simulation results show that the platform can effectively implement the copyright protection of digital video works.

Nisreen I. Yassin (2012): In this paper, a comprehensive approach for digital video watermarking is introduced, where a binary watermark image is embedded into the video frames. Each video frame is decomposed into sub-images using 2 level discrete wavelet transform then the Principle Component Analysis (PCA) transformation is applied for each block in the two bands LL and HH. The watermark is embedded into the maximum coefficient of the PCA block of the two bands. The proposed scheme is tested using a number of video sequences. Experimental results show high imperceptibility where there is no noticeable difference between the watermarked video frames and the original frames. The computedPSNR achieves high score which is 44.097 db. The proposed scheme shows high robustness againstseveral attacks such as JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, and contrast adjustment.

Prachi V. Powar (2013): Objectives of this scheme is to develop low power, robust and secure watermarking system for authentication of video. Here we present an FPGA based implementation of an invisible watermarking encoder. It consists of a watermark generator module and watermark insertion module. The system is initially simulated and tested for various attacks in MATLAB/Simulink and then prototyped on VERTEX-6 FPGA using VHDL. The watermarked video is same as that of original video with an average Peak-Signal-to-Noise Ratio (PSNR) of 46 db.

Methodoogy For Proposed Method

The Proposed Video Watermarking Algorithm This section presents a watermarking algorithm that performs the broadcaster's logo insertion as a visible watermark in the DCT domain. The robustness of DCT watermarking arises from the fact that if an attack tries to remove watermarking at mid-frequencies, it will risk degrading the fidelity of the image because some perceptive details are at mid-frequencies.

ISSN 2349-0292
Impact Factor 2.365

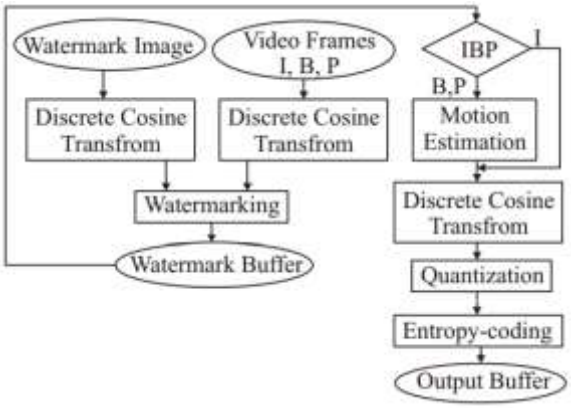

Figure 1: The flow of the proposed watermarking algorithm

The Proposed VLSI Architectures

The data path architecture proposed in this work that can perform watermarking within the MPEG-4 video compression framework uses the components which are discussed in this section. The VLSI architecture for copyright protected MPEG- 4 compression is shown in Figure 3. In the system architecture, the "watermark embedding" module performs the watermarking process. After that procedure, watermarked video frames are obtained. The rest of the units (e.g. entropy coding, zigzag, quantization, DCT, and motion-estimation) of the architecture essentially perform MPEG-4 compression of the video. The system has a controller which generates addressing and control signals to synchronize all components of the system.

Algorithm1:The proposed MPEG-4 watermarking algorithm.

1. Convert RGB colour frames to YCbCr frames for a given host video.
2. Resample YCbCr frames according to 4:2:0 sampling rate.
3. Split Y frame and watermark image into 8 × 8 blocks.
4. Run 2-D DCT for each 8 × 8 block to generate 8 × 8 DCT coefficient matrix.
5. Watermark each 8 × 8 Y DCT matrix with an 8 × 8 watermark DCT matrix.
6. Perform 2-D IDCT for each 8 × 8 watermarked matrix to obtain the pixels.
7. Buffer watermarked Y frame, nonwatermarked and Cr frames for a Group of Pictures (GOP, e.g., 15 continuous adjacent frames).
8. Split the Y frame into 16 × 16 blocks, and Cb and Cr into 8 × 8 blocks.
9. Perform motion estimation for Y frames. Each 16 × 16 Y block is rescaled to 8 × 8 blocks.
10. if (Even first frame (I) of GOP) then
11. return to Step 28.
12. else if (P) Frame then
13. return to Step 17.
14. else if (B) Frame then
15. return to Step 22.
16. end if
17. Perform Y frame forward or backward motion estimation P frames with reference frames (I or P frames). Obtain the motion vectors (MV) and prediction errors of residual frame for motion compensation (MC).
18. if (Y) Frame then
19. return to Step 28.
20. end if
21. Obtain Cb, Cr motion vectors and prediction errors. Go to Step 28.
22. Using bilinear algorithm motion, estimate B frames with two P frames or I and P frames for Y component. Obtain the motion vectors (MV) and prediction errors of residual frame for motion compensation (MC).
23. f (Y) Frame then
24. return to Step 28.
25. else if (Cb and Cr)frames then
26. 26: return to Step 21.
27. end if

28. Perform 2-D DCT on blocks of frames and quantize the 2-D DCT matrix.
29. Zigzag scan quantized 2-D DCT coefficient Matrix.
30. Perform entropy coding of the 2-D DCT coefficients and motion vector.
31. Build structured MPEG-4 stream from buffer.

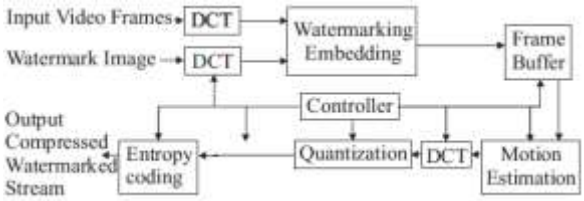

Figure 2: System-level architecture of MPEG-4

Experimental Result

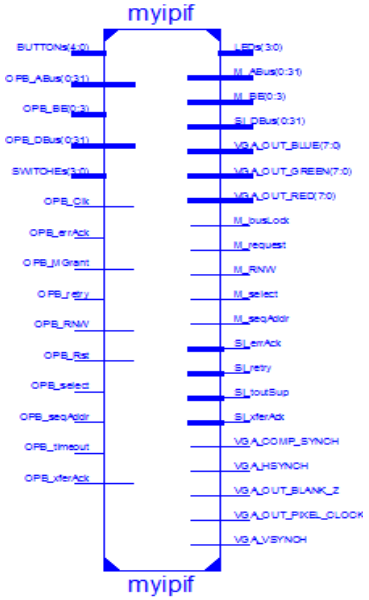

Figure 3. Pin diagram for the overall system generated from RTL schematic.

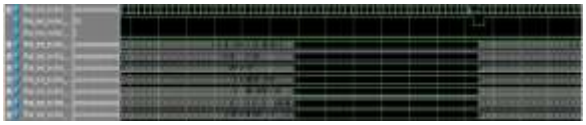

Figure 4 Experimental Simulated Waveforms

Conclusion

In this chapter, we proposed a block based visible image watermarking technique in DCT domain. A single 1D fast 8-point DCT was used to calculate the DCT coefficient of the host image as well as the watermark, which reduces the resource utilization and the power consumption. Twelve pipeline operations were used to increase the speed of the watermark embedding process through temporal parallelism. The proposed system was designed to compute scaling and embedding factors for individual block to improve the perceptual human visual quality. It was implemented on a Xilinx Vertex V technology based FPGA in DSP 48E to analyze the performance and resource utilization. The throughput for the design was calculated and compared with the existing results.

ISSN 2349-0292
Impact Factor 2.365

Reference

1. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing,vol. 6, no. 12, pp. 1673-1687, Dec. 1997.
2. L. Liu, "A survey on digital watermarking technologies", TechnicalReport, Stony Brook University, New York, USA, 2005.
3. I.Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, pp.33-46, July 2001. 552 Waikhom Mona Chanu et al
4. M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in Proc. Security and Watermarking of Multimedia Contents, Jan. 1999, pp. 226–239.
5. Y. J. Zhang, T. Chen, and J. Li, "Embedding watermarks into both DC andAC components of DCT," in Proc. SPIE Security and Watermarking of Multimedia Contents III, Jan. 2001, pp. 424–435.
6. A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-Based watermarkrecovering without restoring to the uncorrupted original image", in IEEEICIP, 1997.
7. R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme forwatermarking images," in IEEE ICIP, 1998.
8. Wai C. Chu, "DCT-Based Image Watermarking Using Subsampling",IEEE Transaction on Multimedia, vol. 5, no.1, March 2003.(P-15).