www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11754-11760

Implementation of a visible and invisible video watermarking technique

K. Shamini, C. Bhagya, M. Sri Sowmya
Department of Electronics and Communication Engineering,
Stanley College of Engineering and Technology for Women

Abstract

Although tremendous progress has been made in the past years on video watermarking, there still exist a number of problems. We believe that the most important one is related to the compression rates, robustness against attacks and high security for privacy data. In digital image processing domain "achieving better compression rates in dual digital watermarking" is still area of concern. The proposed work shows the embedding of visible and invisible watermark during compression on the video encoder and the respective embedding approach on the video is termed as optimized compression/watermarking algorithm and system. The performance of the video watermarking is better when the complexity is low and this low complexity is achieved in our proposed work by discrete cosine transform (DCT). Finally, the results show the high correlation against different attacks in the extraction section. The proposed algorithm is more successful in order to overcome, the conventional algorithm drawbacks and more suitable to applied in the real time applications.

KEYWORDS: Dual video watermarking, DCT, Robustness, Compression rates.

I. INTRODUCTION

The rapid growth of multimedia content in digital form has increased the need to develop secure methods for legal distribution of the digital content. With the speedy growth of the Internet and multimedia systems in distributed environments, it is easier for digital data owners to transfer multimedia documents across the Internet. Therefore, there is an increase in the concern over copyright protection of digital content [1], [6]. Security of digital images has become more and more important with the omnipresence of internet.

The advent of image processing tools has increased the vulnerability for illicit copying, modifications, and dispersion of digital images. Against this background, the data hiding technologies for digital data such as digital watermarking have got a lot of attention recently [49]. Digital watermarking is put into practice to prevent unauthorized replication or exploitation of digital images [35], [21]. Digital watermarking is a technique that provides a way to protect digital images from illicit copying and manipulation. Watermarking is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia element for different purposes such as copyright protection, access control, and broadcast monitoring [13].

A digital watermark is an imperceptible signal added to digital data, called cover work, which can be detected later for buyer/seller identification, ownership proof, and so forth [13]. It plays the role of a digital

signature, providing the image with a sense of ownership or authenticity.

The primary benefit of watermarking is that the content is not separable from the watermark. A watermark is capable of exhibiting numerous significant characteristics. These comprise that the watermark is hard to perceive, endures common distortions, resists malicious attacks, carries numerous bits of information, is capable of coexisting with other watermarks, and demands little computation to insert or detect [39]. In order for a watermark to be useful it must be robust to a variety of possible attacks by pirates.

With the advent of digital video, issues of copyright protection have become more important, since the duplication of digital video signals does not result in the inherent decrease in quality suffered by analog video. A method of copyright protection is the addition of a "watermark" to the video signal. The watermark is a digital code embedded in the video which can be used for the embedded transmission of binary information and which typically indicates the copyright owner. If different watermarks are applied to individual copies of the video, watermarking can also be used to indicate the identity of the legal receiver of each copy.

- **[A] Embedding effectiveness:**The efficiency of a watermarking system lies in the prospectthat the output of the embedder will be watermarked. When input to a detector result in positive detection, the cover work is believed to be watermarked. It is possible to determine the effectiveness of a watermarking system analytically or empirically by embedding a watermark in numerous cover works and identify the watermark [13].
- **[B] Fidelity:**Commonly, the reliability of a watermark system refers to the perceptualresemblance between the original and the watermarked version of the cover work. It is possible to define watermarking system fidelity as a perceptual similarity among the un-watermarked and watermarked works at the point at which they are offered to a viewer [32].
- **[C] Data payload:**Data payload denotes the number of bits a watermark embeds in a unit oftime or works. In case of audio, data payload denotes the number of embedded bits per second that are transmitted. Diverse applications demand diverse data payload. For instance, Copy control applications may necessitate a few bits embedded in cover works [13].
- **[D] Blind or informed detector:**There is a possibility for the informed detectors to demandfor information obtained from the original work rather than original work itself. Conversely, detectors that do not require the original work are referred to as blind detectors. Informed detector provides an enhanced performance in watermark extraction. Nevertheless, this might lead to an enormous number of original works being stored [32].
- **[E] False positive rate:** A false positive is the identification of a watermark from a coverwork which does not contain one in reality. False positive rate denotes the number of false positives anticipated to happen in a given number of runs of the detector. Robustness, security and cost: Robustness denotes the capability to detect the watermarkafter common signal processing operations. Image watermarking should robust to scaling, bending, cropping, lossy compression and the like. Not all applications of watermarking demand all the sorts of robustness. This depends on the nature of application of watermarking system [13], [32].

II. CONVENTIONAL METHOD

Video watermarking is the process of embed ding the copy right information into the frames of the video such that viewer cannot perceive the difference between the original video and watermarked video. This is illustrated in following figure (1)

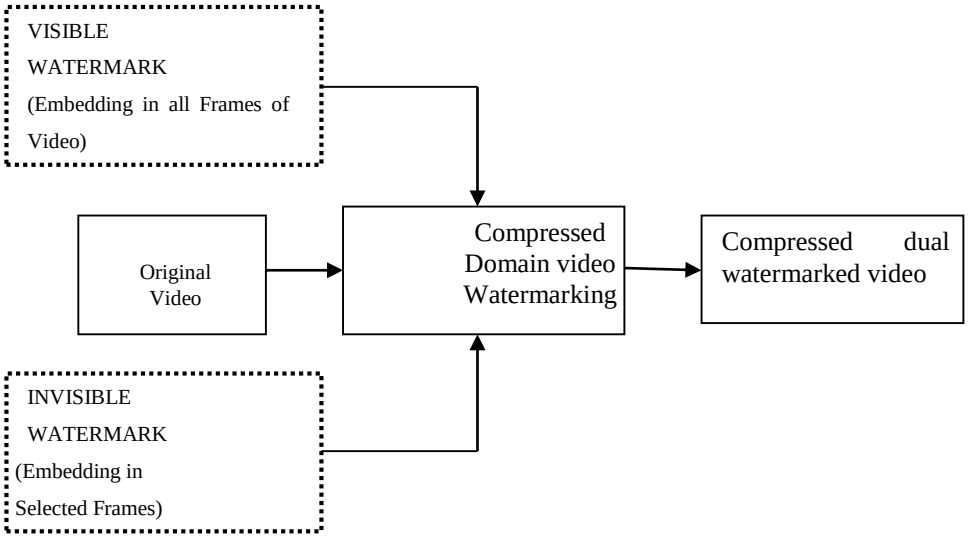


Figure 1:Dual watermarking approach

Integer generator and finally watermark can be easily retrieved by inverting the 0's and 1's of Poisson's integer generator. Simulation results show that recovered watermark has high correlation after different attacks.

III. PROPOSED METHOD

A novel dual watermarking approach is presents in this work and the proposed work main objective is to compress the motion fast video and simultaneously add dual watermark approach. One of the economical strategies for compression is by activity block matching algorithmic program, or motion estimation and motion compensation methodology. The block matching algorithmic program divides this frame and also the previous frame into many macro blocks, scrutiny the blocks within the 2 frames and attempting to look for the most effective matched pairs for every block. Matching criteria is add of Absolute variations (SAD), which is defined as follows:

$$C_{j,k} \sum M \sum M \; abs \; I \; m \; j, n \; k \; Tm, n \; \ldots \ldots \ldots (1)$$

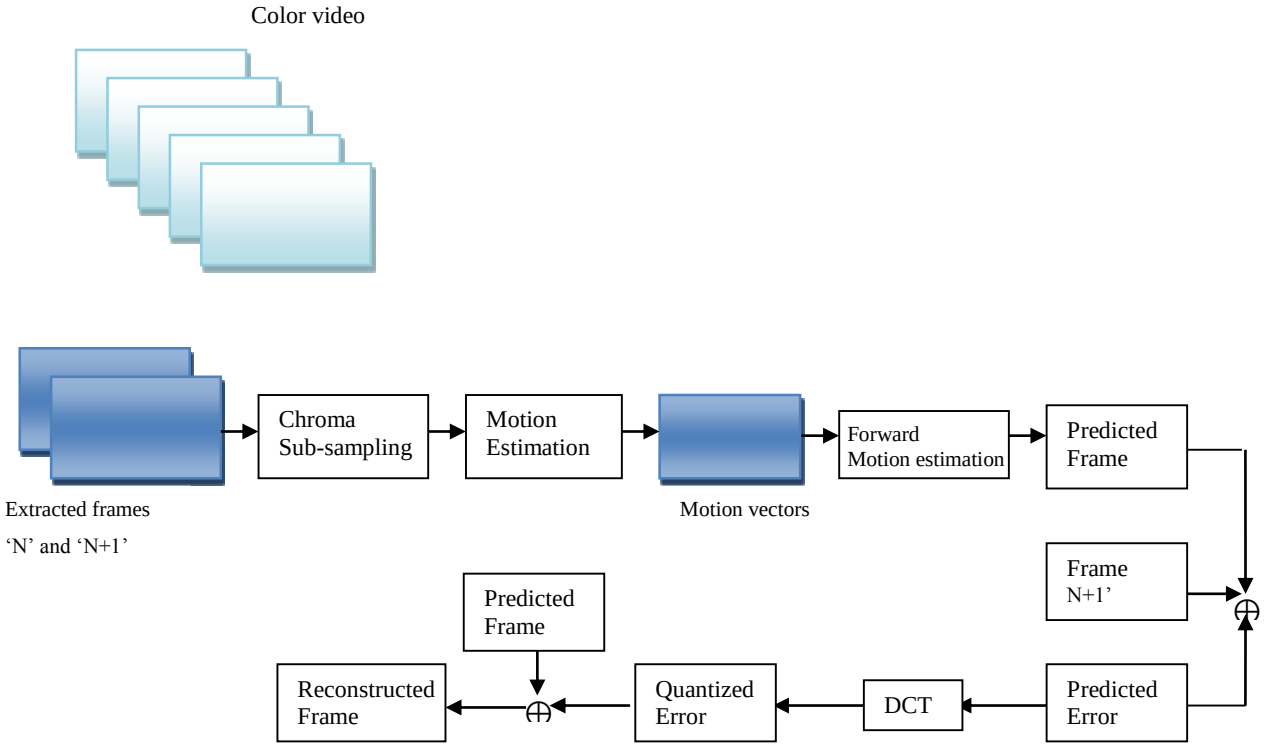


Figure 2: Proposed block diagram

Where I (m, n) is the input macro block and T (Mt, Nt) is the template block values The input image is subtracted from the predictive image, and the differential image is generated. Then, 2 -D DCT is done on each 8 × 8 block of differential image. Add the DCT coefficients of visible and invisible watermarks to host video coefficients as follows If Pg is Poisson integer generator, C (i, j) are host video frame DCT coefficients and W (i, j) are watermark image DCT coefficients, then dual watermarked video frame DCT coefficients are obtained by

If

P g =0, then CW (i, j) =C (i, j) + (βn1 × W1 (i, j))…… (2)

Else,

CW (i, j) =C (i, j) + (βn1 × W1 (i, j) + (βn2× W2 (i, j)) …… (3)

The highlighted portion in the above algorithm gives the novelty involved in designing the system. The Poisson Integer Generator block generates random integers (0 or 1) using a Poisson distribution. The probability of generating a nonnegative integer k is

P= $\lambda^k \exp(-\lambda)/k!$ …… (4)

Where λ is a positive number known as the Poisson parameter The value of initial seed in Poisson generator makes the algorithm to maintain high level security. Where βn1, βn2 are the watermark strength factors of visible and invisible watermark images, which ranges from 0 to 1. Higher the value of βn, more the watermark perceptibility in original

video. The detailed descriptions of other blocks involved in the algorithm like Quantization, Zigzag and Entropy coding modules are given in [14]

IV. RESULTS

Clips (βn2)=0.01	Strength Factor (β_{n1}) =0.1		Strength Factor (β_{n1}) =0.8	
	Compression Ratio (Average)	PSNR (in dB)	Compression Ratio (Average)	PSNR (in dB)
Video1 (46 Frames)	12.11	22.46	11.95	24.32
Video2 (96 Frames)	11.85	28.56	11.63	29.42
Video3 (46 Frames)	12.8	26.44	12.59	28.26

Table 1: Video Quality Metrics

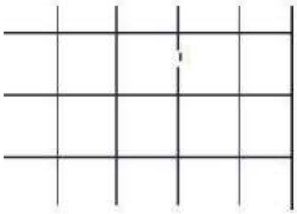


Figure 1: Watermark-1 (visible)

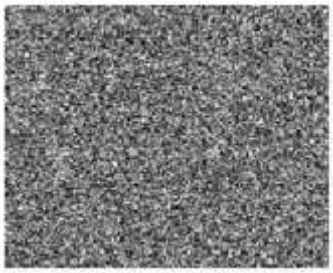
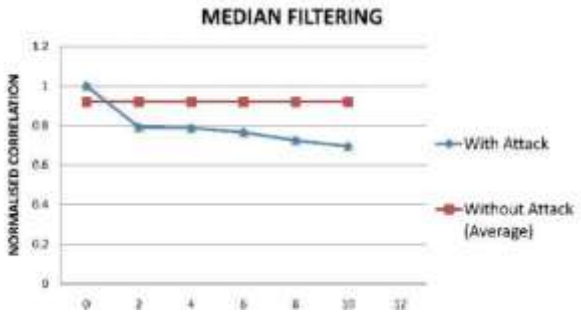


Figure 2: Watermark-2 (invisible)

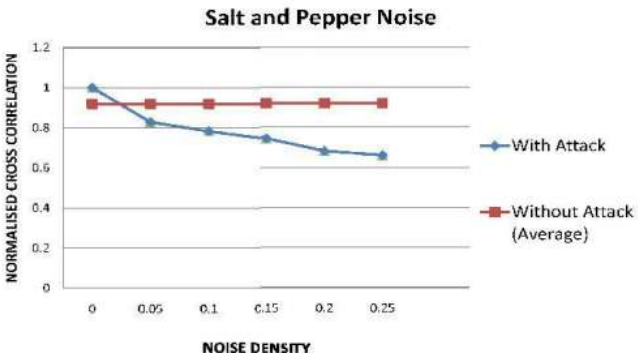
Figure 3: Original video

Figure 4: Dual watermarking for video with ßn1=0.1, ßn2=0.01

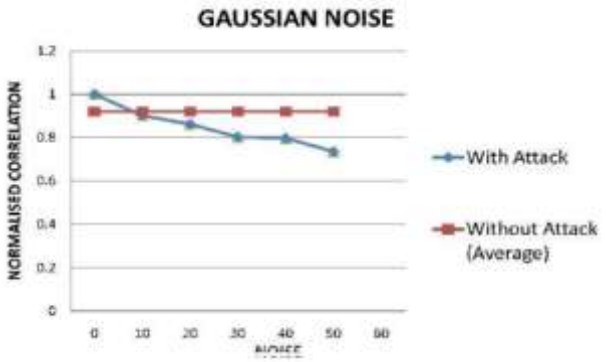
Figure 5: Dual watermarking for video with ßn1=0.8, ßn2=0.01



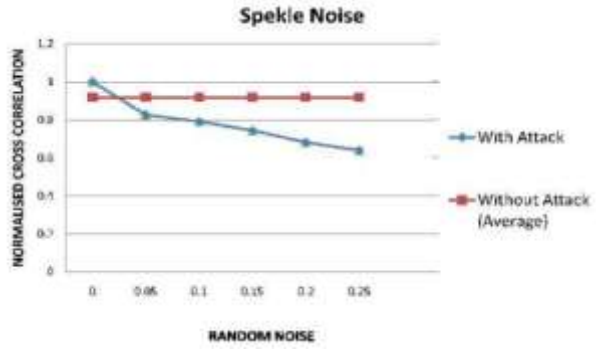
Graph 1: Estimated normalized cross correlation value for different window size median filter operations.



Graph 2: Estimated normalized cross correlation value for different noise density values



Graph 3: Estimated normalized cross correlation value for different noise values



Graph 4: Estimated normalized cross correlation value for different random noises.

V. CONCLUSION

In digital image processing domain "achieving better compression rates in dual digital watermarking" is still area of concern. The proposed work shows the embedding of visible and invisible watermark during compression on the video encoder and the respective embedding approach on the video is termed as optimized compression/watermarking algorithm and system. The performance of the video watermarking is better when the complexity is low and this low complexity is achieved in our proposed work by discrete cosine transform (DCT). Finally, the results show the high correlation against different attacks in the extraction section.

VI. REFERENCES

[1] Y. Hu, S. Kwong, and J. Huang, "Using invisible watermarks to protect visibly watermarked images," in Proc. 2004 Int. Symp.Circuits Syst., vol. 5. pp. 584–587.

[2] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kanakanhalli, "A dual watermarking technique for images," in Proc. 7th ACM Int. Multimedia Conf. (ACMMM), vol. 2. FL,Oct.–Nov. 1999, pp. 49–51.

[3] Frank Hartung, and Bernd Girod. "Watermarking of Uncompressed and Compressed Video," IEE E Transactions on Signal Processing. Vol. 66, No. 3, May 1998, pp. 283 – 302. [4] L. D. Strycker, P. Termont, J. Vandewege, J. Haitsma, A. Kalker, M. Maes, and G. Depovere, "Implementation of a Real-Time Digital Watermarking Process for Broadcast Monitoring on Trimedia VLIW Processor," IEE Proceedings on Vision, Image and Signal Processing, vol. 147, no. 4, pp . 371 –376, Aug 2000.

[5] N. J. Mathai, D. Kundur, and A. Sheikholeslami, "Hardware Implementation Perspective s of Digital Video Watermarking Algorithms," IEEE Transactio ns on Signal Processing, vol. 51, no. 4, pp. 925–938, April 2003.

[6] Y. C. Fan, L. D. Van, C. M .Huang, and H. W. Tsao. "Hardware Efficient Architecture Design of Wavelet-based Adaptive Visible Watermarking," In Proceedings of 9th IEEE International

Symposium on Consumer Electronics, pages 399-403, 2005.

[7] Saraju P. Mohanty, Elias K ougianos, Wei Cai, Manish Ratnani, "VLSI architectures of perceptual based video watermarking for realtime copyright protection," in Proceedings of 10th International Symposium on Quality of Electronic Design, pp.527-534, 2009

[8] S. Biswas, S. R. Das, and E. M. Petriu. "An adaptive compressed MPEG-2 video watermarking scheme," IEEE Transactions on Instrumentation and Measure ment, 54(5):1853-61, Oct 2005.

[9] L. Qiao and K. Nahrstedt."Watermarking Methods for MPEG Encoded Video: Towards Resolving Rightful Ownership," In Proceedings of the IEEE International Conference on Multimedia Computing and Systems, pages 276-285, 1998.

[10] S. P. Mohanty, N. Ranganathan, and R. K. Namballa. "VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S2DC) Design," IEEE Transactions on Very Large Scale Integration Systems, 13(8):10 02-1012, August 2005