

Video Watermarking Algorithm Resilient to MPEG-2 Compression and Collusion Attacks

Rogelio Reyes, Clara Cruz, Mariko Nakano, Héctor Pérez

SEPI ESIME Culhuacan, National Polytechnic Institute of México
Av. Santa Ana 1000 Col. San Francisco Culhuacan, CP 04430, México, City. MÉXICO
rreyesre@ipn.mx, mariko@calmecac.esimecu.ipn.mx

Abstract. A video watermarking algorithm for digital video with blind extraction resilient to MPEG-2 Compression and several attacks is presented in this paper. In practice, the robustness depends on the watermark embedding energy used, which is limited by the media degradation caused by the watermark. Reliable embedding algorithms must assure watermark persistence up to an extreme quality downgrading. The proposed algorithm embeds binary visually recognizable pattern, such as owner's logotype, in DWT domain of some randomly selected video shots. To increase security, watermark data is disordered by chaotic mixing method before its embedding. The main advantage of the algorithm is its simplicity, blindness and robustness. Extensive experimental simulations demonstrate the watermark imperceptibility and robustness against several video degradations and attacks. Also we show that extracted watermark data from watermarked video sequence in blind manner is sufficiently clear after several attacks.

Video Watermarking Algorithm

First the host video is segmented into video sequences, and then some of them are selected randomly for watermark embedding. The following steps are repeated for each frame of the selected video sequence: Perform a two dimensional DWT based on the Daubechies-wavelet on each selected frame of the luminance channel. The multilevel decomposition is processed until the first level. Then the watermark is embedded into the LL_1 subband. Watermark embedding is based on magnitudes of the wavelet coefficients; disordered watermark image by chaotic mixing method [1] is adaptively spread spectrum and embedded into these coefficients. Wavelet coefficients are divided into blocks with size 3x3 pixels, then a mean of the block is computed. Watermark bit is embedded by changing the center coefficient value of each block with the corresponding modified value. The watermarked video is obtained computing the inverse DWT of the modified wavelet coefficient frames in the luminance channel. As mentioned above each watermark data is related to the static and dynamic composition in the video sequence offering better robustness to malicious attacks.

To extract the watermark, the original unmarked video and original watermark data are not required. Again, the process starts with the two dimensional wavelet decomposition of the luminance channel of selected frames of each video sequence selected in embedding scheme. Applying DWT, we can retrieve the LL_1 coefficients. Wavelet coefficients are divided in blocks with size 3x3 pixels, and then a mean of the block is computed, extract the center coefficient value of each block, and to obtain the corresponding value of the pixel in these block calculate a mean of the disordered watermark embedded in each frame of the selected sequences. The reconstructed watermark image can be obtained through the two keys used by chaotic mixing method in the watermarking preprocessing section.

Experimental Results

The proposed algorithm has been evaluated using well-known video sequences “Foreman”, “carphone” and “bus”. These sequences are in the YUV color space in terms of one luma and two chrominance components, and their size are 288×352 (CIF format). The watermark is a binary image with size 48×48 . In the experiments we use 21 frames of 250 in these sequences to embed a watermark image.

We have conducted some experiments to evaluate the robustness of our proposed watermarking algorithm [2]-[4]. For this purpose, we have performed some of the classical sequence manipulations including: noise attack, frame dropping, frame swapping, collusion attacks and MPEG-2 Compression. For collusion attack a large number of frames are modified via linear combination with independent watermark patterns. An example of such an attack is frame averaging, its compute the average of the two nearest neighbors’ frames to replace the actual frame. In the experiments, we have tested 10 times each video sequence, in which the results are average values of independent experiments. The performance of video watermark approach is calculated in terms of normalized correlation between original watermark and reconstructed watermark. Figure 1 demonstrates good robustness against noise contamination, MPEG-2 compression and frame attacks. In all analyzed attacks, normalized correlation values between original watermark and extracted one is higher than 0.85, which indicates that the extracted watermark image is very clear after watermarked video sequence is attacked.

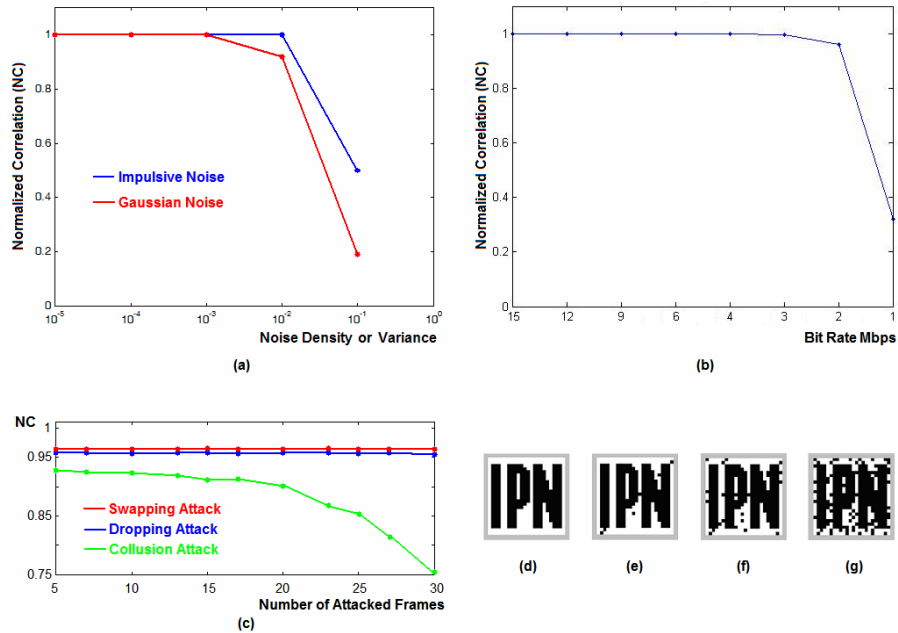


Fig. 1. Normalized Correlation Curves: (a) robustness to Impulsive and Gaussian noise with different noise densities and variances respectively, (b) robustness to MPEG-2 Compression with different bit rate, (c) robustness to frame swapping, dropping, and averaging, (d) original watermark, (e)-(g) extracted watermarks with $NC=0.9792$, $NC=0.9021$ and $NC=0.7326$ respectively.

We compare the proposed algorithm with different schemes [4]-[8]. The results are shown in Table 1, 'O' means that the embedded watermark is robust against attack, 'N' means not showed and 'X' means that embedded watermark can not be recovered correctly or this kind of attack was not proved.

Table 1. Performance comparison of the proposed scheme.

	MPEG-2 Bit Rate Supported	Frame Attack			Noise Contamination	
		Collusion	Dropping	Swapping	Impulsive	Gaussian
Our scheme	2 Mbps	O	O	O	O	O
Zhuang [4]	N	O	O	O	O	X
Zhao [5]	N	O	O	O	X	X
Zhang [6]	N	X	O	O	O	O
Liu [7]	2 Mbps	O	O	X	X	X
Fan [8]	2 Mbps	X	O	X	X	O

Conclusions

The video watermarking algorithm here presented is robust to various common attacks. This approach allows us to exploit the advantages of the DWT and Chaotic Mixing to improve invisibility and robustness of the visual recognizable watermark, such as logotype. The extraction process performs without original video sequence and original watermark data and extracted watermark image doesn't have any ambiguity.

Acknowledgments. This work is supported by the National Polytechnic Institute of México and National Council for Science and Technology of Mexico.

References

1. G. Voyatzis and I. Pitas.: Embedding Robust Watermarks by Chaotic Mixing. In: Proceedings of Conf. Int. Digital Signal Processing, Vol. 1. 1997. 213-216.
2. M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, G. F. G. Depovere, and J. Haitzma.: Digital watermarking for DVD video copy protection. In: IEEE Signal Processing Magazine, Vol. 17. Sep. 2000. 47-57.
3. M. D. Swanson, B. Zhu, and A. H. Tewfik. Multiresolution Scene-Based Video Watermarking Using Perceptual Models. In: IEEE Journal on Selected Areas in Communications. Vol. 16. May 1998. 540-550.
4. H. Zhuang, Y. Li and C. Wu.: A Blind Spatial-temporal Algorithm Based on 3D Wavelet for Video Watermarking. In: IEEE International Conference on Multimedia and Expo. (ICME) , vol. 3, 2004. 1727-1730.
5. Z. Zhao, N. Yu and X. Li: A Novel Video Watermarking Scheme in Compressed Domain Based of Fast Motion Estimation. In: IEEE Int. Conf. on Communication Technology (ICCT). 2003. 1878-1882.
6. J. Zhang, J. Li, and L. Zhang.: Video Watermark Technique in Motion Vector. In: XIV Brazilian Symposium on Computer Graphics and Image Processing. 2001.
7. L.S. Liu, R.H. Li, Qi. Gao: A Robust Video Watermarking Scheme Based on DCT . In: Proceedings of the 4th Int. Conf. on Machine Learning and Cybernetics, August 2005.
8. L. Fan, F. Yanmei.: A DWT-Based Video Watermarking Algorithm Applying DS-CDMA. In: IEEE TENCON 2006, November 2006.