IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 4 (Mar. - Apr. 2013), PP 46-50
www.iosrjournals.org

A Video Watermarking Scheme to Hinder Camcorder Piracy

Aditya.J, HarinniyIlanchezhian, Anoop.M

Department Of Information Technology Sri Venkateswara College Of Engineering Sriperumbudur- 602105 Tamil Nadu, India.

Abstract: *A watermarking technique that hinders camcorder piracy in Theaters by implementing the playback control is set forth. In this technique we watermark a finite number of frames so that any acquiescent video player cannot play the video. The watermarking technique should be impervious to any kind of geometric alterations and it should be a lossless compression, which will prevent the re-recorded video to be played in any of the video players.The IWT is not only computationally faster and more memory-efficient but also more suitable in lossless data-compression applications. The IWT enables you to reconstruct an integer signal perfectly from the computed integer coefficients. This method is not only simple to implement but is also more efficient than the other proposed watermarking techniques.*

I. Introduction

While all kinds of piracy are a thorn in the side of the movie industry, when illicit movies appear on the Internet at the same time as theatrical releases, camcorder piracy particularly draws the ire of studios. Over the past decade an awful lot of money has been spent trying to mitigate the problem. One of the methods used in avoiding the camcorder piracy was the theater camcorder jamming system[1], but did not prove to be very efficient. For the past few years, watermarking techniques have been used to resolve this problem. Messages are embedded into watermarks and any acquiescent video player will detect this watermark and follow the restrictions that are encoded in the watermark.

For a little more than a decade, watermarking techniques have been designed to, among other purposes, control access to digital content [2]. In the case of a playback control application, the watermark embedded in the video sequence is designed to provide information on whether video players are authorized to display the content or not [3]. Compliant devices detect the watermark and obey the encoded usage restrictions.
Controlling access to media content that was re-recorded with a camera inside a movie theater is a challenging problem. To begin with, the recorded video might be a slightly resized, rotated, and cropped version of the original content. Furthermore, these copies are also subjected to video compression. Since the original content is not available during the decoding process (i.e., it is a blind procedure), extracting the watermark is not a straightforward task. The decoding process must, to a certain extent, be robust to some geometric distortions (rotation and scaling), as well as cropping and lossy compression.

Several watermarking methods that are robust to common geometric distortions have been presented. For example, in [4], an image watermarking method based on the Fourier–Mellin transform is proposed. The scheme is robust to rotation and scaling but weak to distortions caused by lossy compression.
Another algorithm is presented in [5]. The watermark is embedded into a 1-D signal, which is obtained by taking the Fourier transform of the image, resampling it into log-polar coordinates, and integrating along the radial dimension. The method is ro- bust to rotation, scaling, and translation. However, the scheme cannot withstand cropping.

In [6], two watermarks are employed. The first one is used to embed the message while the second one, a 0-b watermark, is employed as a geometric reference. This reference watermark is embedded in the spatial domain which results in low robust- ness. Information hidden in the space domain can be easily lost to quantization, which makes the watermarking scheme vulnerable to lossy compression and other attacks. Once the reference watermark has been changed, the decoder assumes that there is no watermark embedded in the content and, therefore, does not search for the hidden message.

A content-based image watermarking method is offered in [7], where robustness to geometric attacks is achieved using feature points from the image. This scheme is shown to be successful to certain attacks, but the watermark detection process is computationally intensive and, therefore, may not be practical for real-time video applications.

II. IWT and SVD

Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra by many renowned mathematicians. SVD has many practical and theoretical values; Special feature of SVD is that it can be performed on any real (m, n) matrix. Let's say we have a matrix *A* with *m* rows and *n* columns, with rank *R and* $R \leq n \leq m$.

Then the *A* can be factorized into three matrices:
$A = USV^T$

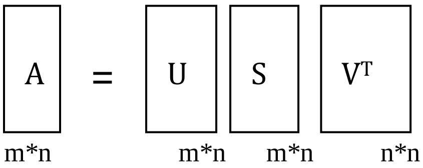

Fig 1:General SVD manipulation matrices

Let A be a general real matrix of order m × n. The singular value decomposition (SVD) of A is the factorization:

$A = U * S* V^{T}$

Where U and V are orthogonal (unitary) and S = diagonal ($\sigma_1, \sigma_2, ..., \sigma_r$), where σ_i, i = 1(1)r are the singular values of the matrix A with r = min(m, n) and satisfying

$\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r$

The first r columns of V the right singular vectors and the first r columns of U the left singular vectors.

A. SVD Approach for Image Compression

Image compression deals with the problem of reducing the amount of data required to represent a digital image. Compression is achieved by the removal of three basic data redundancies:

1) Coding redundancy, which is present when less than optimal;
2) Inter pixel redundancy, which results from correlations between the pixels;
3) Psycho visual redundancies, which is due to data that is ignored by the human visuals.

The property of SVD tells us “the rank of matrix A is equal to the number of its nonzero singular values”. In many applications, the singular values of a matrix decrease quickly with increasing rank. This propriety allows us to reduce the noise or compress the matrix data by eliminating the small singular values or the higher ranks.

When an image is SVD transformed, it is not compressed, but the data take a form in which the first singular value has a great amount of the image information. With this, we can use only a few singular values to represent the image with little differences from the original.

To illustrate the SVD image compression process, we show detail procedures:

$A=USV^T=\sum_{i=1}^{r} \sigma_i u_i v_i^T$

That is *A* can be represented by the outer product expansion:

$A= \sigma_1 u_1 v_1^T + \sigma_2 u_2 v_2^T + \ldots + \sigma_r u_r v_r^T$

When compressing the image, the sum is not performed to the very last Singular values (SV), the SVs with small enough values are dropped. (Remember that the SVs are ordered on the diagonal.)

The closet matrix of rank *k* is obtained by truncating those sums after the first *k* terms:

$A_k= \sigma_1 u_1 v_1^T + \sigma_2 u_2 v_2^T + \ldots + \sigma_k u_k v_k^T$

The total storage for *k A* will be
k (m+n+1)

The integer *k* can be chosen confidently less then *n,* and the digital image corresponding to *k A* still have very close the original image. However, they chose the different *k* will have a different corresponding image and storage for it. For typical choices of the k, the storage required for *k A* will be less the 20 percentage. In this project, experiment and testing for different k are carried out.

B. Image Compression Measures

To measure the performance of the SVD image compression method, we can computer the compression factor and the quality of the compressed image. Image compression factor can be computed using the Compression ratio:

CR = m*n/ (k (m + n + 1))

C. Integer Wavelet Transform

According to [11], every wavelet or subband transform associated with finite length filters can be obtained as the Lazy wavelet followed by a finite number of primal and dual lifting steps and a scaling (the Lazy wavelet essentially splits the signal into its even and odd indexed samples). By combining the lifting constructions with rounding-off in a reversible way, a wavelet transform that maps integers to integers can be obtained. For example, the integer-to-integer wavelet transform that approximates Le Gall 5/3 filters is given by,

$$d_{l,n} = s_{0,2n+1} - [1/2(s_{0,2n} + s_{0,2n+2}) + 1/2],\ s_{1,n} = s_{0,2n} + [1/4(d_{1,n-1} + d_{1,n}) + 1/2] \qquad (1)$$

where *sj;n* and *dj;n* are the *nth* low-frequency and highfrequency wavelet coefficients at the *jth* level, respectively [11]. When *j* = 0, *s*0*;n* represents the *nth* pixel value itself. The function *bxc* rounds *x* to the nearest integer towards minus infinity. To make transforms nonexpansive, symmetric extension compatible with invertible integer-to-integer wavelet
transforms [12] is used.

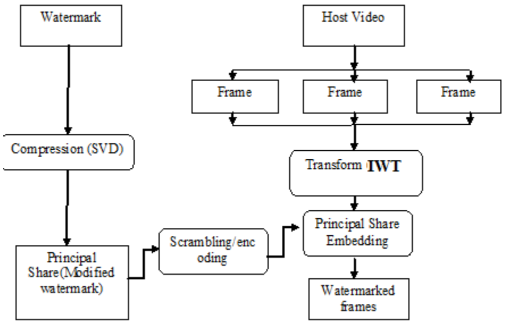

Fig 2. Block Diagram of SVD implementing IWT

III. Experimental Results

The proposed algorithm is demonstrated using MATLAB. We have taken 8-bit gray scale tree image as host image of size 256 x 256 and for primary and secondary watermark, we have used 8-bit gray scale lena image and boy image of sizes 128 × 128 and 64 × 64 respectively. The secondary watermark is embedded into primary and the watermarked primary is encrypted. For encryption, chaos encryption technique is used.

For embedding the encrypted watermarked primary into the host image, we have used 2-level of decomposition using Daubechies filter bank. For extracting both the watermarks, decryption is done using the chaos technique. The decrypted image is then used to extract the primary watermark and this is used for extracting the secondary watermark. In figures 2 and 3 all original, watermarked images and extracted watermarks are shown.

To investigate the robustness of the algorithm, the watermarked image is attacked by Average and Median Filtering, Gaussian noise addition,Resize and Rotation . After these attacks on the watermarked image, we compare the extracted watermarks with the original one.

To investigate the robustness of the algorithm, the watermarked image is attacked by Average and Mean Filtering, JPEG and JPEG2000 compression, Gaussian noise addition, Resize, Rotation and Cropping. After these attacks on the watermarked image, we compare the extracted watermarks with the original one. The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio).

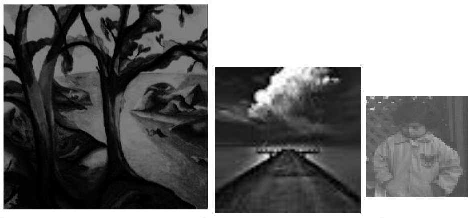

Fig. 3. Original Images a) Host image b) Primary watermark c) Secondary watermark

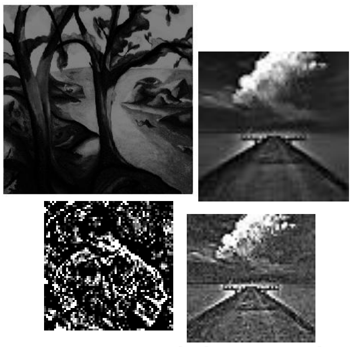

Fig. 4. Watermarked and extracted watermark images a) Watermarked Host image b) Watermarked Primary watermark c) Extracted Secondary watermark d) Extracted Primary watermark

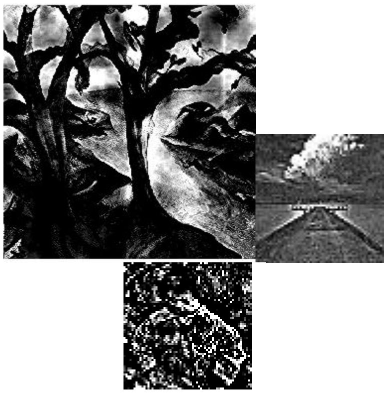

Fig. 5. Median filtering Attack a) Recovered Host image b) Extracted Primary watermark c) Extracted Secondary watermark

IV. Conclusion

This paper deals with a novel dual watermarking scheme, which includes encryption, to improve rightful ownership, protection and robustness. An image encryption algorithm based on logistic map is proposed. A well-designed chaos-based stream cipher can be a good candidate and may even outperform the block cipher, on speed and security. In this, the key stream generator is based on coupled chaotic logistic maps that one logistic chaotic system generates the random changing parameter to control the parameter of the other. The watermarked primary image is encrypted using the chaos based encryption technique. Later it is embedded in the cover image and transmitted. The chaotic encryption scheme supplies us with a wide key space, high key sensitivity, and the cipher can resist brute force attack and statistical analysis. It is safe and can meet the need of image encryption.

For the extraction of watermark, a reliable watermark decryption scheme and an extraction scheme is constructed for both primary and secondary watermark. Robustness of this method is carried out by variety of attacks.

References

[1] Mot. Picture Assoc. Amer., 2007. [Online]. Available: http://www.mpaa.org/piracy.asp.

[2] P. B. Schneck, “Persistent access control to prevent piracy of digital information,” *Proc. IEEE*, vol. 87, no. 7, pp. 1239–1249, Jul. 1999.

[3] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufmann, 2002.

[4] J. J. K. O’Ruanaidh and T. Pun, “Rotation, scale and translation invariant digital image watermarking,” in *Proc. Int. Conf. Image Processing*, 1997, pp. 536–539.

[5] C.-Y. Lin, M.Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, “Rotation, scale, and translation resilient watermarking for images,” *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767–782, May 2001.

[6] C. V. Serdean, M. A. Ambroze, M. Tomlinson, and J. G.Wade, "DWTbased high-capacity blind videowatermarking, invariant to geometrical attacks," *Proc. Inst. Elect. Eng., Vis., Image Signal Process.*, vol. 150, pp. 51–58, Feb. 2003.

[7] P. Bas, J. M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, no. 9, pp. 1014–1028, Sep. 2002.

[8] Z. Dawei, C. Guanrong, and L.Wenbo, "A chaos-based robust waveletdomainwatermarking algorithm," *Chaos, Solitons Fractals*, vol. 22, pp. 47–54, 2004/10.

[9] P. W. Chan, M. R. Lyu, and R. T. Chin, "A novel scheme for hybrid digital video watermarking: Approach, evaluation and experimentation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 12, pp. 1638–1649, Dec. 2005.

[10] N. Kingsbury, "Image processing with complex wavelets," *Philos. Trans. Math., Phys., Eng. Sci.*, vol. 357, p. 2543, 1999.

[11] A. R. Calderbank, I. Daubechies, W. Sweldens, and B. L. Yeo, "Wavelet transforms that map integers to integers," *Applied and Computational Harmonics Analysis*, vol.5, no. 3, pp. 332-369, 1998.

[12] Michael D. Adams and Rabab K. Ward, "Symmetric-extensioncompatible reversible integer-to-integer wavelet transforms," *IEEE Trans. Signal Processing*, vol. 51, no. 10, Oct. 2003.

[13] P. Loo and N. Kingsburry, "Digital watermarking using complex wavelets," in *Proc. Int. Conf. Image Processing*, 2000, pp. 29–32.

[14] P. Loo and N. Kingsbury, "Digital watermarking with complex wavelets," in *Proc. Inst. Elect. Eng. Seminar Secure Images Image*