A CONTENT BASED WATERMARKING SCHEME USING RADIAL SYMMETRY TRANSFORM AND SINGULAR VALUE DECOMPOSITION

Lakehal Elkhamssa¹ and Benmohammed Mohamed²

¹LAMIE laboratory, Department of Computer Engineering, Batna University, Algeria lakehal_elkhamssa@yahoo.fr ²LIRE laboratory, Department of Computer Engineering, Constantine University, Algeria ben_moh123@yahoo.com

ABSTRACT

The Watermarking techniques represent actually a very important issue in digital multimedia content distribution. To protect digital multimedia content we embed an invisible watermark into images which facilitate the detection of different manipulations, duplication, illegitimate distributions of these images. In this paper we present an approach to embedding invisible watermarks into color images using a robust transform of images that is the Radial symmetry transform. The watermark is inserted in blocs of eight pixels large of the blue channel using the Singular Value Decomposition (SVD) of these blocs and those of the radial symmetry transform. The blue channel is justified when we know that many works states that the human visual system is less sensible to perturbation in the blue channel of the image. Results obtained after tests show that the imperceptibility of the watermark using this approach is good and its robustness face to different attacks leads to think that the proposed approach is a very promising one.

KEYWORDS

Image watermarking, Singular value decomposition, Radial symmetry transform, Invisible watermarking

1. INTRODUCTION

Nowadays, multimedia content is largely used, due to the progressive development of new imaging techniques and devices. Users of these techniques and devices share generally these contents over communication channels that can be unsecure. This wide transmission of image content make it easily modified. These modifications disregard generally author's ownership that is gradually in danger because of this situation. So the multimedia content protection became a rigorous need to defend the author's copyright and to protect multimedia content from different illegal manipulations.

DOI: 10.5121/csit.2014.4106

As a response to this need of protection come the digital watermarking of multimedia contents [1], [2]; which is no other than information hidden in the multimedia content such that a slight modification on the content results in a modification of the information hidden which is considered as a sign of unauthorized content's manipulation. A survey of watermarking techniques can be found in [3].

2. RELATED WORK

The watermarking method presented here belongs to the second generation ones. In such approaches image content is used in digital watermarking throw the insertion of the watermark in specific points of image like points of interest, edges, corners or other features [4]. A featurebased watermarking scheme was first proposed in [5] where the authors use the Mexican Hat wavelet scale interaction to extract features in the image that can resist a series of attacks which makes them suitable to be used as emplacement to insert and to extract the watermark. Another content-based approach in [6] uses a reworked copy of the traditional Harris corner detector. The reworked copy calculates the corner response function within a circular window originate from the image centre and covers the largest area of it to resist image centre based rotation attacks. The new detector gives geometrically significant points that can detect possible geometric attacks. We find in [7] the use of interest points from the Harris corner detector to watermark synchronization before the extraction to recover the watermark positions that can be changed during a geometrical To do, authors generate points of interest using the Harris detector after scale attack. normalization in order to get the most stable points in the image by avoiding the sensitive character of the Harris detector face to scale changes. Then they search within a circular region around the detected points whether the detector response of a selected point reaches a local maximum or not. If it is the case they consider the point, otherwise they neglect it. After that they profit from the characteristic of Pseudo Zernike Moments magnitude which is invariant to rotation to design the watermark to embed in a rotation invariant pattern.

Another work [8] uses the robustness of interest's points to select the positions of the insertion which strengthen the relationship between the watermark and the image content. The detection of interest's points makes possible the creation of triangular partitions of the image and afterward the insertion of the watermark in each triangle. We note that image content is also used in watermarking systems in order to resist other geometric attacks like scale changing and translation in [9].

The watermarking system proposed in this paper uses image content through singular value decomposition (SVD). The use of SVD in watermarking schemes is not recent; we find in literature many watermarking schemes based on SVD decomposition [10], [11]. The SVD decomposition may be used in spatial or frequency domain. In frequency domain, the SVD decomposition can be combined with lifting wavelet transform like in [12]; it is also possible to combine it with the discrete cosines transform (DCT) as in [13] or many other transformations. The contribution of this work is the use of an SVD decomposition of a strong content transform (radial symmetry transform) to insert in the blue channel where the red and the green channels are just used to synchronize the detection of the watermark.

3. SCHEME OVERVIEW

3.1. Imperceptibility and Robustness

To be invisible to human visual eye, first, the mark is inserted in the blue channel, which is the one to which the human visual system is less sensitive [14]. Second, the watermark bits are

inserted in points of high interest in the image; those points with high luminance values make the modifications in the image imperceptible. That is the property of imperceptibility which mast marks any consistent watermarking scheme; the other property is the robustness of the system [15]. The robustness of our scheme is achieved by using robust transform of image information. This transform is called radial symmetry transform and it presents very good robustness against image transformations and nosing. The radial symmetry transform is originally used to detect image features [16], [17].

3.2. The Radial Symmetry Transform

Author in [18] details an algorithm to calculate the radial symmetry transform of an image. With this approach a symmetry score is calculated from votes of one pixel to surrounding pixels. The transform is calculated in one or more radii n. the value of the transform at radius n indicates the contribution to radial symmetry of the gradients a distance n away from each point.

At each radius n, an orientation projection image O_n and a magnitude projection image M_n are formed. These images are generated by examining the gradient g at each point p from which a corresponding positively-affected pixel $p_{+ve}(p)$ and negatively-affected pixel $p_{-ve}(p)$ are determined, as shown in Fig. 1. The positively-affected pixel is defined as the pixel that the gradient vector g (p) is pointing to, a distance n away from p, and the negatively-affected pixel is the pixel a distance n away that the gradient is pointing directly away from.

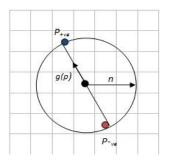


Figure 1. Positively and negativelly affected pixels

Coordinates of the positively-affected pixel are given by:

$$p_{+ve} = p + ROUND\left(n \cdot \frac{g(p)}{\|g(p)\|}\right)$$
(1)

Coordinates of the negatively-affected pixel are given by:

$$p_{-ve} = p - ROUND\left(n \cdot \frac{g(p)}{\|g(p)\|}\right)$$
(2)

The orientation and magnitude projection images are initially zero. For each pair of affected pixels, the corresponding point p_{+ve} in the orientation projection image O_n and magnitude projection image M_n is incremented by 1 and ||g(p)||, respectively, while the point corresponding to p_{-ve} is decremented by these same quantities in each image. That is:

Computer Science & Information Technology (CS & IT)

(4)

(7)

$$O_n(p_{+ve}(p)) = O_n(p_{+ve}(p)) + 1$$
 (3)

$$O_n(p_{-ve}(p)) = O_n(p_{-ve}(p)) - 1$$

$$M_{n}(p_{+ve}(p)) = M_{n}(p_{+ve}(p)) + ||g(p)||$$
(5)

$$M_{n}(p_{-ve}(p)) = M_{n}(p_{-ve}(p)) - ||g(p)||$$
(6)

The radial symmetry contribution at radius n is defined as the convolution:

$$\mathbf{S}_{n} = \mathbf{F}_{n} * \mathbf{A}_{n} \tag{7}$$

Where:

$$F_n(p) = \frac{M_n(p)}{k_n} \left(\frac{\left| \tilde{O}_n(p) \right|}{k_n} \right)^{\alpha}$$
(8)

And
$$\tilde{O}_n(p) = \begin{cases} O_n(p) & \text{if On} < \text{kn} \\ k_n & else \end{cases}$$
 (9)

 A_n is a two-dimensional Gaussian, α is the radial strictness parameter, and k_n is a scaling factor that normalizes M_n and O_n across different radii.

The full transform is defined as the average of the symmetry contributions over all the radii considered:

$$S = \frac{1}{|N|} \sum_{n \in N} S_n \tag{10}$$

4. THE PROPOSED SCHEME

The proposed algorithm inserts the watermark bits into the blue channel of the image based on an SVD decomposition of this channel. The SVD decomposition used here is a bloc based one which necessitates the decomposition of the blue channel into blocs of 8 pixels large in different locations in the image the locations are objects centres obtained after a local maxima search over the radial symmetry transform.

At the same time we should calculate the symmetry transform using the red and green channel of the original image. The symmetry transform is also divided into blocks in the same locations as the blue channel and with the same size.

4.1. Insertion of the watermark

To insert the pixel of the binary watermark we need to calculate the *svd* of both, the blue block i and the symmetry transform of the block i as indicated in Figure 2. The insertion mechanism uses the formula:

$$\sigma_{bk} = W_i * \sigma_{sk} * \alpha \tag{11}$$

Where *k* is the index of the singular value which holds the watermark.

 α is the embedding strength (an adjustment parameter between the quality and the robustness). It is chosen experimentally.

 σ_{bk} , σ_{sk} are respectively singular values from the range of big singular values of the blue bloc and those of the radial symmetry transform bloc.

4.2. Extraction of the watermark

Figure 3 presents the extraction scheme; it is based on the decomposition of blue image channel and radial symmetry transform into blocs, then the decomposition of each bloc to its singular values.

To extract the watermark we use the singular values following the formula:

$$\widetilde{W}i = \sigma_{bkw} / \sigma_{skw} / \beta$$

Where β is $1/2\alpha$, σ_{bkw} and σ_{skw} are respectively singular values from high singular values of the blue blocs and those of the radial symmetry transform blocs of watermarked image

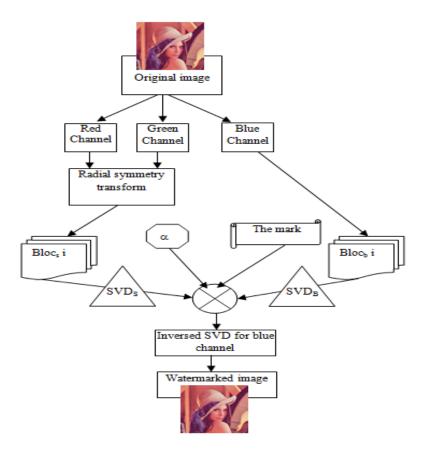


Figure 2. The mark insertion scheme

5. RESULTS AND DISCUSSION

In this section we present results of tests of imperceptibility and robustness for our scheme. To test our watermarking scheme we use an image database composed of color images of size 512×512 pixels: Lena, baboon, air plane, peppers. The mark used is a binary image of size 8×8 pixels.

Figure 4 presents the original images used in tests with the watermark image to the right bottom of the figure.

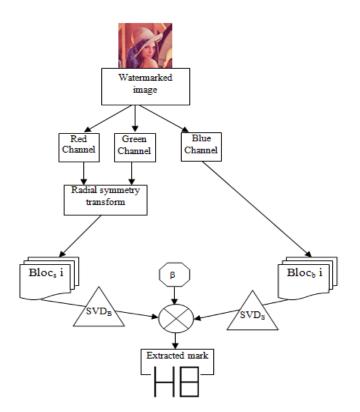


Figure 3. The mark extraction scheme

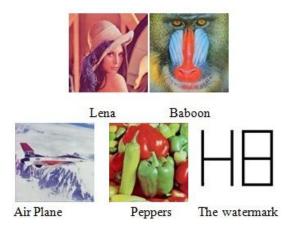


Figure 4. Test images with the watermark used

The table 1 presents the imperceptibility results according to tree objective measures: PSNR (Peak Signal to Noise Ratio) calculated between the original image and the watermarked one, NC (Normal Correlation) and BCR (Bit Correct Ratio) calculated between the original watermark and the extracted one.

We note that the results obtained with the PSNR measure between original image and the watermarked one are very good when we know that authors considered a PSNR rate as good when it is greater than 30dB. With tested images we have PSNR from 42 to 46dB.

When investigating table 1 we find that the NC measure is between 0.97 and 1 when the BCR measure is between 98.44% and 100%. These are very interesting rates which indicates that the proposed algorithm makes a high-quality extraction of the watermark.

To evaluate the robustness of our algorithm we should test its performance face to different attacks. The attack chosen are common in watermarking algorithm evaluation and includes low pass filtering, noise, jpeg compression and cropping. In this paper, we have used attacks with different parameters to check as deeply as possible the robustness of the proposed algorithm. Attacks used to test our watermarking system are given in table 2.

In this paper we have not tested the capacity of our proposed scheme, but we claim that our algorithm has a very good capacity since it inserts watermark bits into radial symmetry transform local maxima.

Image	PSNR	NC	BCR%	
Lena	+ 46.13 dB	1	100	
Baboon	+ 42.76 dB	0.97	98.44	
Air Plane	+ 45.42 dB	0.97	98.44	
Peppers	+ 45.42 dB	1	100	

Table 1. imperceptibility and robustness of the watermark in absence of attacks.

Table 2. Attacks used in different tests.

	Attacks	Parameters
SP1	Salt & Pepper noise	Density 0.008
SP2	Salt & Pepper noise	Density 0.002
SP3	Salt & Pepper noise	Density 0.05
GN1	Gaussian noise	M=0.0 V=0.001
GN2	Gaussian noise	M=0.1 V=0.001
GF	Gaussian filter	3x3
SH	Sharpening	3x3
HE	Histogram equalization	
MF	Median filter	3x3
JC1	JPEG Compression	Quality 80
JC2	JPEG Compression	Quality 60
CR	Cropping	1/8 of image
AF	Average filter	3x3
LF	Laplacian filter	3x3
Rot1	Rotation	0.2°

60

Table 3 presents the NC and BCR measure between the watermark inserted and the one extracted using our extraction scheme with different attacks over four test images.

By observing the interval of these two objective measures over all attacks (NC between 1 and 0.62, BCR between 100% and 71.88%) we can deduce that the proposed algorithm perform well face to these attacks. Furthermore, the robustness of the method is related to the tested image, thus to the content. Then, enhancing the content transform may enhance the extraction. The robustness of the algorithm face to the rotation attack can be reinforced using a robust rotational radial symmetry transform.

In the next figures (5-9) we present comparison graphics of NC rates between watermarks extracted with our algorithm and those presented in reference [12].

Algorithm in [12] uses gray scale images of 256 x 256 pixels where the watermark image is a binary image of 32×32 pixels which represents the letter "A".

N°	Lena		Baboon		Air plane		Peppers	
	NC	BCR%	NC	BCR%	NC	BCR%	NC	BCR%
SP1	0.88	89.06	0.97	98.44	1.00	100	1.00	100
SP2	1.00	100	0.97	98.44	0.97	98.44	1.00	100
SP3	0.73	71.88	0.90	78.13	0.90	79.69	0.73	75.00
GN1	1.00	100	0.97	98.44	1.00	100	0.97	98.44
GN2	1.00	100	0.97	96.88	0.97	98.44	0.97	98.44
GF	1.00	100	0.97	98.44	0.97	98.44	1.00	100
SH	1.00	93.75	0.97	98.44	1.00	100	0.97	98.44
HE	1.00	100	0.97	98.44	0.91	95.31	0.84	92.19
MF	0.90	95.31	0.82	90.63	0.77	87.50	0.71	82.81
JC1	1.00	100	0.93	96.88	1.00	100	0.84	92.19
JC2	0.81	90.63	0.73	87.50	0.94	96.88	0.63	81.25
CR	0.93	95.31	0.98	98.44	0.93	95.31	1.00	100
AF	0.85	92.19	0.73	84.38	0.66	79.69	0.62	78.13
LF	0.71	85.94	0.90	95.31	0.90	95.31	0.80	90.63
Rot1	0.90	93.31	0.84	92.19	0.85	92.19	0.81	90.63

Table 3. Robustness of the proposed scheme (NC and BCR) over different attacks

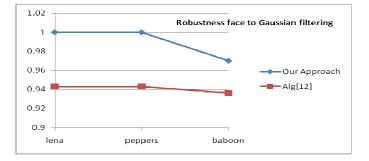
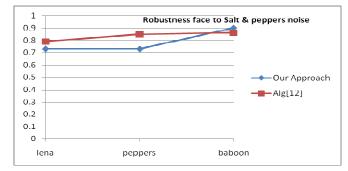
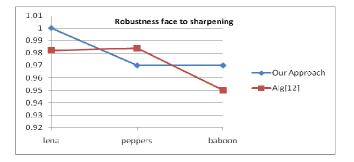


Figure 5. Comparaison of NC rates face to gaussian filtering

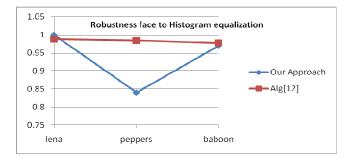
Computer Science & Information Technology (CS & IT)













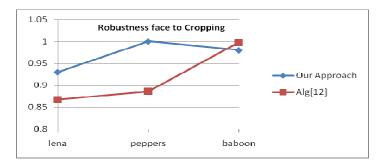


Figure 9. Comparaison of NC rates face to cropping attack

6. CONCLUSION AND FURTHER WORKS

The watermarking algorithm presented in this paper is a promised one since it presents good results in term of robustness and imperceptibility. However, the approach necessitates to be compared to other works in order to be judged correctly. To this day there are no works which evaluate different content based algorithms face to different attacks. So the comparison of this work with other works should be based on the same attacks and considering the same metrics. Since it is the case, we resolve, in our future work, to evaluate and to compare the present work with other content based watermarking techniques using a unified testing benchmark.

ACKNOWLEDGEMENTS

Lakehal elkhamssa thanks Pr. Noui L. for his inestimable aid and considers his contribution to success this work.

REFERENCES

- [1] I. Cox, M. Miller, and J. Bloom. "Digital Watermarking: Principles & Practices". Morgan Kaufmann Publisher, San Francisco, USA, 2002.
- [2] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications," IEEE Signal Processing Magazine, pp. 33-46, 2001.
- [3] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 3rd international conference on industrial informatics (INDIN), 2005.
- [4] M. Kutter, S. K. Bhattacharjee, T. Ebrahimi, "Towards second generation watermarking schemes", international conference on image processing, 1999.
- [5] C. W. Tang and H. M. Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Transactions on Signal Processing, Vol. 51, pp. 950-959, 2003.
- [6] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," Signal Processing , Vol. 87, pp. 1264-1280, 2007.
- [7] L.D. Li, B. L. Guo AND L. Guo, "Combining Interest Point and Invariant Moment for Geometrically Robust Image Watermarking", Journal of information science and engineering, vol. 25, pp. 499-515, 2009.
- [8] P. Bas, J.M. Chassery, B. Macq, "Toward a content-based watermarking scheme", Journal of signal processing [journal de Traitement du Signal], vol. 19, pp. 11-17, 2002.
- [9] D. Simitopoulos, D.E. Koutsonanos, M.G. Strintzis, "Robust Image Watermarking Based on Generalized Radon Transformations", IEEE Trans. on Circuits and Systems for Video Technology, IEEE, vol. 13, pp. 732-745, 2003.
- [10] R. Liu and T. Tan, "A svd-based watermarking scheme for protecting right-ful ownership", IEEE Transactions on Multimedia, vol. 4, pp. 121-128, 2002.
- [11] C. Bergman, J. Davidson, "Unitary Embedding for Data Hiding with the SVD", Security, Steganography, and Watermarking of Multimedia Contents VII, SPIE vol. 5681, 2005.
- [12] K. Loukhaoukha, "Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective", Phd thesis, Laval University, pp. 115-126, 2010.
- [13] F. Huang, Z. H. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR", Pattern Recognition Letters, vol. 25, pp. 1769–1775, 2004.
- [14] R. W. G. Hunt, The reproduction of color. Fountain press, Tolworth, England, 1988.
- [15] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," Proceedings of the IEEE, vol. 87, pp. 1079-1107, 1999.
- [16] G. Heidemann, "Focus of Attention from Local Color Symmetries" IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 26, pp. 817-830, 2004.
- [17] A. Rebai, A. Joly, N. Boujemaa, "Constant Tangential Angle Elected Interest Points," in Proc. of the 8th ACM International Workshop on Multimedia Information Retrieval (MIR), pp. 203-211, 2006.
- [18] A. Zelinsky, G. Loy, "Fast Radial Symmetry for Detecting Point of Interest," IEEE Trans. on Pattern Analysis and Machine Intelligence, pp. 959-973, vol. 27, August 2003.

62

AUTHOR

Lakehal elkhamssa is currently a researcher in the LAMIE laboratory, Batna University, Algeria. She received his Magister degree in computer science in the University of Batna in 2009. Her main research interests are: image watermarking, image understanding and colour constancy.

