Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wavelet Based Fingerprinting Scheme for Image Sharing

Kanchan S. Tule
M.E Digital Electronics
Government Residencial Women's Polytechnic
Yavatmal, India

C. N. Deshmukh
Asst. Professor (EXTC Deptt)
PRMIT&R,
Badnera, India

Abstract: ***At present due to vast use of internet for exchanging data. Many pirated data are uploaded on internet thus data piracy has become a serious concern. Thus Digital Fingerprinting technique is proposed for multimedia content distribution in peer to peer (P2P) network and help multimedia content provider by improving copy-right protection. In this paper, a new method is introduced for fingerprinting an image. The proposed method uses wavelet and Principal Component Analysis (PCA) techniques for fingerprint generation. Fingerprinting is done in two phases. During, first phase wavelet technique is used to obtain low frequency representation of the test image. In second phase, PCA finds the features of the representation. Set of fingerprint matrices can be created based on a proposed algorithm. Finally, each matrix combined with the low frequency representation to become a unique fingerprinted matrix. Size of the fingerprinted image is very small but it has most important information. Without this information, quality of the reconstructed image is very poor.***
We have used different wavelet types for fingerprint generation for a natural image and an artificial image and find best wavelet type based on the performance.

Keywords— Digital Fingerprinting, Mean square error (MSE), PSNR, Discrete Wavelet Transform and principal component analysis (PCA)

I. INTRODUCTION

The recent growth of networked multimedia systems have increased the need for the protection of digital media. To protect and enforce the intellectual property rights Copyright protection need to be enhanced. Copyright protection involves the authentication of image ownership and the identification of illegal copies of a (possibly forged) image. Techniques are needed to prevent the copying, forgery and unauthorized distribution of images and data. Without such methods, placing images or data sequences on a public network puts them at risk of theft and alteration. An approach to secure the authorized media sharing in Peer-to-Peer (P2P) networks, is embed an unique-mark (fingerprint) into each authorized copy in P2P networks so that it can be used to track the pirate initiator. This study also proposes another scheme for protecting the ownership of digital media files that have been circulated without copyright mark embedded. To protect this type of files, the ownership of each file needs to be stored associated with its meta-data (such as the ownership, title, and artist) and can be identified correctly later on. Since the size and the number of the media files to be stored are extremely large, the mini versions (fingerprints) of the files become necessary to be derived. The common criteria of designing these two approaches are to ensure the fingerprint is compact, robust, discriminative. The whole design consists of the fingerprint generation, embedding, distribution, verification. The proposed scheme has utilized the concept of watermarking by embedding an unique watermark into each individual copy of the original media file before distribution. First, the wavelet technique obtains a low frequency representation of the media file and the PCA technique finds the features of the representation. After that, a set of fingerprint matrices can be created based on a proposed algorithm. In this paper, a digital fingerprinting technique for an image file based on wavelet and principal component analysis (PCA) is proposed.

II. LITERATURE REVIEW

Literature survey shows that very few researchers have worked on fingerprinting for P2P applications so far. Tsolis et al. proposed their watermarking scheme recently for P2P application. There are multiple keys as the watermark is cast into the image by the pseudorandom sequence of a gaussian distribution generator. However, the paper did not mention the robustness of the scheme against common attacks [1]. Many researchers have proposed algorithms mainly for watermarking and among those watermarking schemes, there are two main streams: the one which embed a watermark directly in the spatial domain and the others which implement it in a frequency domain. It is found that the transform domain watermarking schemes are typically much more robust to image manipulation as compared to the spatial domain schemes [2].

Among the schemes applying wavelet techniques, Kaarna et al. proposes an algorithm in the PCA and wavelet transform domain. They first applied PCA to produce eigen images and then decomposed them into multi resolution images. Correspondingly, the watermark image is also decomposed into a multi resolution image in same scale. Finally, the human visual system (HVS) as the strength parameter is adopted for watermark embedding. The scheme is applicable for embedding one mark because of the uniqueness of the strength parameter [3]. Liu et al. Have proposed their

algorithm based on singular value decomposition (SVD). The host image is originally presented as USV^{-1}, where the matrix S contains the singular values and U,V are singular vectors. The algorithm adds the watermark to the singular values S. Thus, the modified singular value is presented by $U_w S_w V_w^{-1}$. Then the newly generated singular value S_w will replace the original S to generate the watermarked image. The singular vectors U_w and V_w are kept by the owner just for watermark detection. Since S_w approximately equal to S, the visual quality of the image is preserved. To extract the watermark, the watermarked image will be decomposed again using SVD. The main issue of this method is that the attacker can also claim his/her watermark easily by providing another set of singular vectors . It proves that embedding a fingerprint only on singular values is unreliable[4]. Hien et al. also proposed a PCA method. The difference is they embed the watermark into the eigenvectors. First, the PCA process decomposes the image into eigenvectors and eigen values. Then the image is projected onto each eigenvector and becomes a coefficient matrix. The watermark is embedded into the coefficient matrix based on the selected components. Finally, the watermarked image is obtained by applying the inverse PCA process. The robustness becomes the issue of this method. Because the eigenvectors are normalized, the numerical value of each component of the eigenvector is very small and can be easily corrupted by distortion methods [5]. Some research group uses wavelet and PCA techniques as features were utilized to detect the image information [6] [7].

The proposed fingerprinting technique is illustrated in Section III, and its results are compared in Section IV. Section V discusses the conclusion and future scope.

III. PROPOSED SYSTEM

The proposed technique has Decomposd the source file is into two parts: base file and supplementary file. The base file then will carry the embedded unique fingerprint for each peer and be distributed using the traditional server–client mode. while the supplementary file will be freely distributed in P2P networks. Fig. 1 shows the structure of the fingerprint distribution using unique key.

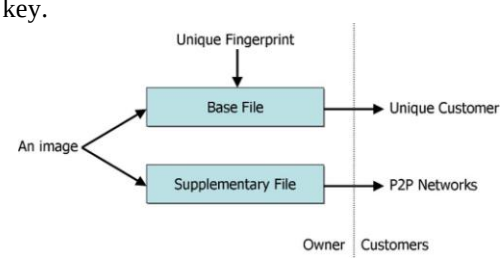

Fig. 1 Fingerprint distribution

- ***Fingerprint Generation***

In our approach, the base file will be distributed from the central server to all the clients.So it should be designed to have small size but contain the most important information. Thus, the load of the server can be alleviated to some extent, while the supplementary file can be larger but contains less important information. By doing this, the peer who has the supplementary file has no commercial motivation to leak the supplementary file alone because of its low quality without the base file. One possible approach to derive a small size base file is to decompose the image into two parts, the base pixel matrix and the detail pixel matrix. The base pixel matrix can give us a rough outline of the image. Since the base pixel matrix has higher correlation information, its entropy value is small so that it can be compressed into a very small size with no quality loss. Here wavelet and PCA techniques are employed for fingerprint generation and embedding .

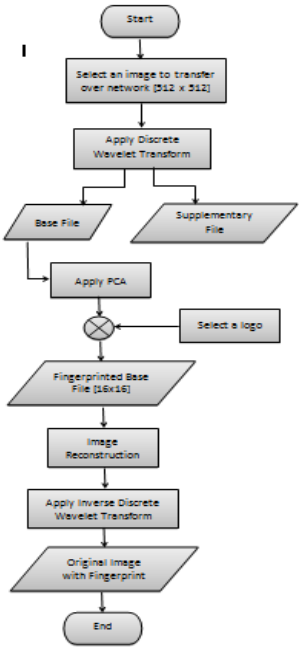

Fig. 2 Fingerprint generation

Fig. 2 shows the flowchart of the fingerprint generation and embedding.

The original image is decomposed into two coefficients which are approximation and detailed coefficients. PCA is carried out on the approximation coefficients. PCA is added with the secret key to generate the fingerprinted image. Size of fingerprinted image is very small but contains important information. To recognize the embedded fingerprint, the receiver needs to decompose the fingerprinted image some level using the wavelet technique.

- ***Decomposition***

Wavelets are mathematical functions that cut up data into different frequency components and then study each component with a resolution matched to its scale. They have advantages over traditional Fourier methods in analysing physical situations where the signal contains discontinuities and sharp spikes. In wavelet transform, an image is split into one approximation (also called approximation coefficient) W_{ac} and three details in horizontal, vertical, and diagonal directions which are named W_{hc} (or horizontal coefficient), W_{vc} (vertical coefficient), and W_{dc}(diagonal coefficient). The approximation is then itself split into a second-level approximation and details, and the process is repeated. For a 5-level decomposition, the approximation and the details are described in (1)

For 5-level decomposition, the approximation and the details are described in equation 1.

$w_{acJ} = [Img, A_J]$
$w_{hcj} = [Img, Hj]$ j = 1, 2, 3,4,5
$w_{vcj} = [Img, Vj]$ j = 1, 2, 3,4,5
$w_{dcj} = [Img, Dj]$ j = 1, 2, 3,4,5 ----------(1)

Where Img denotes the input image and A_J, H_j, V_j and D_j are approximation, horizontal, vertical and diagonal coefficients. For image decomposition, even the size of the coefficients in a different level is different, but the coefficients are still a 2-D matrix. Equation (2) indicates how the image is recovered:

$$Img = a_j + \sum_{j=1}^{j} d_j$$
$$= Wac_j A_j + \sum_{j=1}^{j} Whc_j H_j + \sum_{j=1}^{j} Wvc_j V_j + \sum_{j=1}^{j} Wdc_j D_j \quad \text{----------(2)}$$

j = 1,2,3,4,5

Where Img is the reconstructed image and d_j is the detailed coefficients.

In this method, the fingerprint is small but strong and robust compared to the multimedia file. In this paper, we have implemented the fingerprint method on both the gray scale and color images. First, the host image with size 512 * 512 was decomposed into the five levels by different discrete wavelet transform. For fifth-level decomposition, the coefficient set is W= [w_{ac5}, w_{hc5}, w_{vc5}, w_{dc5}, w_{hc4}, w_{vc4}, w_{dc4}, w_{hc3}, w_{vc3}, w_{dc3}, w_{hc2}, w_{vc2}, w_{dc2}, w_{hc1}, w_{vc1}, w_{dc1}].At the fifth level, the size of the approximate coefficient is significantly reduced from original to 16 * 16. This coefficient is called from now on as the base file .Correspondingly; the other coefficients are defined as the supplementary file.

- ***Principal Component Analysis (PCA)***

The approximation coefficient at the fifth level was then used to calculate its principals. It goes through three steps according to the following equations:

BF'= BF-avg(BF) ----------(3)
BF"= cov (BF', BF'^{T}) ----------(4)
BF"V= VD ----------(5)

Where V and D are the set of eigenvectors and the set of Eigen values of BF".

There are a total of 16 eigenvectors which make up the columns of V. It is represented as;

$V= [\vec{V}_{16}|\vec{V}_{15}|.....|\vec{V}_{1}]$ ----------(6)

Where the eigenvectors are arranged in descending order according to their principal components and each eigenvector is a 16 * 1 vector. Equation (7) illustrates how the fingerprint matrix is derived.

$$FPM_{mat}^{pre} = L *(\vec{S}*\vec{V}^{T}) \quad \text{----------(7)}$$

Where a scale vector defined as $\vec{S}$, which is a 16×1 vector, is multiplied with L and one of the eigenvectors, for instance $\vec{V}_m$ (m=1,2….16). L is a visually meaningful full matrix with all positive elements, and only known by the source owner. Thus, it can be a company's logo, another low resolution of a portion of the original host image or simply a portion of the host image. It is utilized to prove the right ownership fingerprint. The elements of S can be viewed as the coefficient of the fingerprint amplitude. The bigger the values of S, the more visible a distortion the fingerprint creates; the smaller the values of S, the weaker the fingerprint energy will be. The value S_i(i=1,2,…..,16) in the scale vector is chosen on the basis of empirical optimization. T indicates the transpose operation. *full* denotes the transformation operation of the non reversible matrix to reversible matrix by fine tuning the singular value matrix of the nonreversible matrix. After the multiplication, the matrix size is 16×16 which is the same as L. Also, even the data items in each column have different magnitudes. Fine adjustments on each element are done, so that the obvious boundary between columns is invisible. This procedure can be modelled as (11). We call the procedure *Column Unify*, because the fine adjustment coefficients from c_{1j} to c_{nj} are created to adjust all the elements in the 5th column of matrix FPM_{mat}^{pre} to have the same value. The rule of unification not only ensures that the value keeps the sign as before but also maintains a certain difference between two

columns. To prevent the previous steps of implementation from creating visual distortion, the variation of the whole matrix was limited by a perceptually lossless threshold. Thus, the scale vector and the fine adjustment coefficients should be adjusted accordingly. The generated fingerprint matrix is named FP_{mat}.

FP_{mat} = Column Unify $[FPM_{mat}^{pre}]$

$= \text{diag}[c_{11}, c_{21}, \ldots, c_{n1}] [FPM_{mat}^{pre}]_{COL1}$

$+ \text{diag}[c_{12}, c_{22}, \ldots, c_{n2}] [FPM_{mat}^{pre}]_{COL2}$

$+ \ldots + \text{diag}[c_{1n}, c_{2n}, \ldots, c_{nn}] [FPM_{mat}^{pre}]_{COLn}$

FP_{mat} as well as BF are then added to average of BF, and the fingerprinted image can be reconstructed based on the fingerprinted fifth approximation matrix BF (alternatively called the fingerprinted base file) using an inverse DWT. Under the unification operation, the robustness of the fingerprint is enhanced. Because the absolute magnitude of elements in each column is replaced by one value, the sign of each column is kept which means the discrimination feature between columns is maintained.

- ***Fingerprint Detection***

A Since only the owner, e.g., the media producer keeps the mapping between the fingerprint and the customer, as long as the producer successfully tracks back the fingerprint for a suspect data, for example, the pirate customer can be revealed. The suspected data is defined as a data which is freely distributed out of the scope of owners' authorized P2P networks.
In our case, to identify the embedded fingerprint, the multimedia producer needs to decompose the fingerprinted image into five levels using the wavelet technique so that a 16*16 approximate 512*512 matrix is obtained .

IV. SIMULATION RESULTS

For a given image. Pre-processing has been done i.e. conversion of image into grey level image. Proposed method's are followed to obtain best correlation between input image and reconstructed fingerprinted image. Here images are decomposed up to 5 levels using different discrete wavelets. Principal components are calculated on the approximation coefficients of last level. The decomposed images were reconstructed using different respective inverse discrete wavelet tharnsform. In this section we are considering 2 images one is natural and other artificial image. We are comparing result of these two images using different discrete wavelet types.

[A]. RESULTS FOR NATURAL IMAGE

Fig.3. a) Original image b) Reconstructed image(db1)

Fig.4. a) Original image b) Reconstructed image(db6)

Fig.5. a) Original image b) Reconstructed image(sym1)

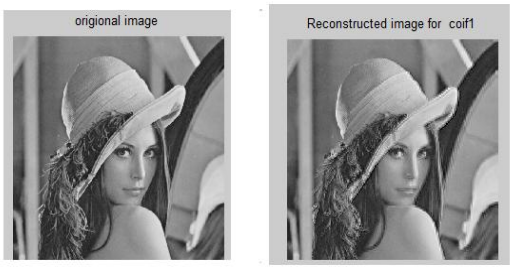

Fig.6. a) Original image b) Reconstructed image(coif1)

Fig.7. a) Original image b) Reconstructed image(bior1.1)

Fig.8. a) Original image b) Reconstructed image(haar)

[B].RESULTS FOR ARTIFICIAL IMAGE

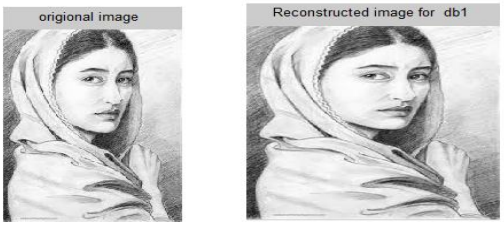

Fig.9. a) Original image b) Reconstructed image(db1)

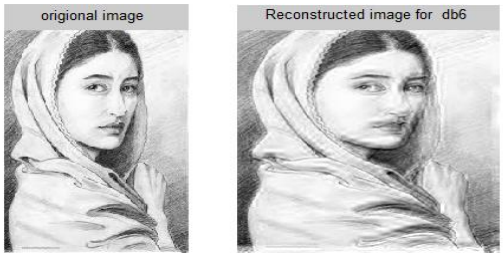

Fig.10. a) Original image b) Reconstructed image(db6)

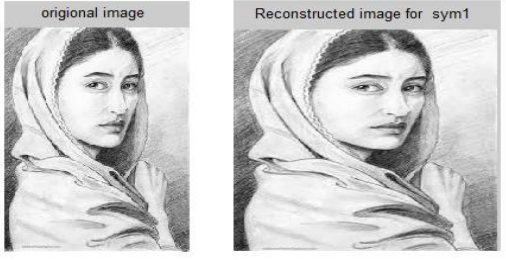

Fig 11. a) Original image b) Reconstructed image(sym1)

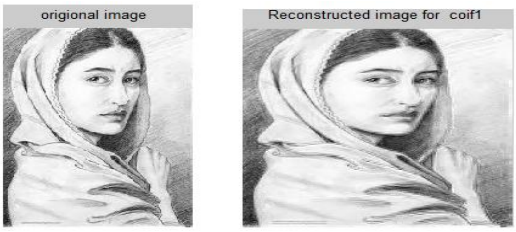

Fig.12. a) Original image b) Reconstructed image(coif1)

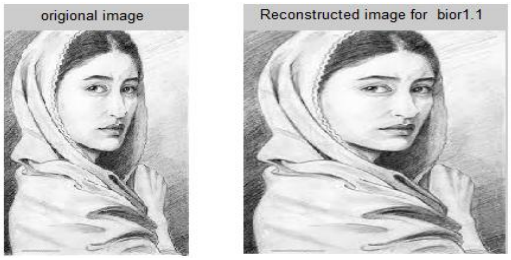

Fig.13. a) Original image b) Reconstructed image(bior1.1)

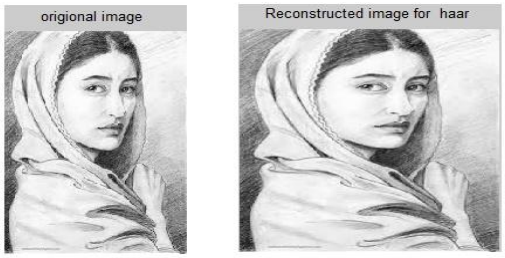

Fig.14. a) Original image b) Reconstructed image(haar)

For best reconstruction, Mean Square Error (MSE) value should be low , Peak Signal-to-Noise Ratio (PSNR) and correlation between original and reconstructed images should be high. The below table1. has shown correlation obtained for natural and artificial image between original and reconstructed image are good for all discrete wavelet types. Thus metric is based on MSE and PSNR value of reconstructed image. By comparing PSNR and MSE values for all wavelets it is found that for a natural image 'sym1' has low MSE value and high PSNR value and 'db2' has high MSE value and low PSNR value . Similarly for an artificial image, 'bior1.1' has low MSE value and high PSNR value and 'db2' has high MSE value and low PSNR value .

Hence the result shows that, for a natural image 'sym1' gives more superior output than other discrete wavelet types. 'db2' gives inferior result among all discrete wavelet types.

For an artificial image, 'bior1.1' gives more superior output and 'db2' gives inferior result among all discrete wavelet types.

Table 1. Comparison of MSE and PSNR value for natural and artificial image

Sr. No.	Wavelet Type	(Natural image		Correlation	Artificial image		Correlation
		MSE	PSNR		MSE	PSNR	
01	DB1	0.1680	55.8785	0.99997	0.6832	49.7854	0.99986
02	DB2	811.1896	19.0396	0.9998	724.9692	19.5276	0.99992
03	SYM1	0.1211	57.2996	0.99998	0.4254	51.8424	0.99992
04	COIF1	267.9493	23.8503	0.99977	249.8778	24.1535	0.99986
05	BIOR1.1	0.2539	54.0841	0.99995	0.2460	54.2220	0.99996
06	RBIO1.1	0.1836	55.4922	0.99996	1.0535	47.9045	0.99978
07	HAAR	0.2656	53.8881	0.99995	0.6947	49.7125	0.99987

V. CONCLUSION

In this paper, in order to achieve robustness and scalability for a natural image and an artificial image, fingerprinting generation and detection scheme is used .This scheme uses discrete wavelet transform to decompose image in order to achieve low frequency representation of image which gives strong robustness similarly PCA(Principal Component Analysis) is used to extract feature representation of fifth level approximation coefficient by determine orthogonal eigenvector. In this scheme PCA technique is applied on small size matrix (fifth level approximation coefficient) which causes low computation complexity.

Fingerprint generation of a natural image and an artificial image are done using different discrete wavelet transform and PCA mechanism then the image are reconstructed using appropriate inverse discrete wavelet transform.

Thus the metric is based on MSE(mean square error) value and PSNR(peak signal to noise ratio) value of reconstructed image. For better performance MSE value should be low and PSNR value should be high.

REFERENCES

[1] D. Tsolis, S. Sioutas, and T. Papatheodorou, "Digital watermarking in Peer to Peer networks," in *16th Int. Conf. Digital Signal Processing*, Greece, pp. 1–5, Jul. 2009.

[2] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," in *Proc. Int. Conf. Image Processing, 1998 (ICIP 98)*, vol. 2, pp. 419–423, Oct. 4–7, 1998.

[3] A. Kaarna and P. Toivanen, "Digital watermarking of spectral images in PCA/wavelet-transform domain," in *Proc. IEEE Int. Geoscience and Remote Sensing Symp., 2003 (IGARSS '03)*, vol. 6,pp. 3564–3567, Jul. 21–25, 2003

[4] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp.121–128, Mar. 2002.

[5] T. D. Hien, Z. Nakao, K. Miyara, Y. Nagata, and Y. W. Chen, "A new chromatic color image watermarking and its PCA-based implementation," in *ICAISC 2006, LNAI 4029* , pp. 787–795, 2006.

[6] E. Chang, J. Wang, C. Li, and G. Wiederhold, "RIME: A replicated image detector for the world wide web," in *SPIE Multimedia Storage and Archiving Systems III*, Bellingham, VA, pp. 58–67, Nov. 1998.

[7] M. Sanchez, X. Binefa, J.Vitria, and P. Radeva, "Local color analysis for scene break detection applied to TV commercials recognition," in*Proc. Int. Conf. Vis. Inf. Syst*,, pp. 237–244, 1999 .

[8] D. S. Milojicic, V. Kalogeraki, R. Lukose, K. Nagaraja, J. Pruyne, B. Richard, S. Rollins, and Z. Xu, Peer-to-Peer Computing Hewlett- Packard Company [Online]. Available: http://www.hpl.hp.com/techre-ports/2002/HPL- - 57R1.pdf , 2002.

[9] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of Peer-to-Peer overlay network schemes," in *IEEE Communications Survey and Tutorial*, Mar. 2004

[10] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.

[11] D. G. Lowe, "Object recognition from local scale- invariant features," in *Proc. ICCV* , pp. 1150–1157, 1999.

[12] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Special Issue on Enabling Security Technologies for Digital Rights Management, Proc. IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[13] E. T. Lin, C. I. Podilchuk, T. Kalker, and E. J. Delp, "Streaming video and rate scalable compression: What are the challenges for watermarking?," in *Proc. SPIE Int. Conf. Security and Watermarking of Multimedia Contents III*, San Jose, CA, Jan. 22–25, vol. 4314, 2001.

[14] Dittmann, "Combining digital watermarks and collusion secure fingerprints for customer copy monitoring," in *Proc. IEEE Seminar Sec. Image & Image Auth.*, pp. 128–132, Mar. 2000.

[15] M. Kutter, S. Bhattacharjee, and T. Ebrahimi, "Towards second gen-eration watermarking schemes," in *Proc. IEEE Int. Conf. Image Processing (ICIP 99)*, Kobe, Japan, vol. 1, pp. 320–323, 1999.

[16] Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[17] T. D. Hien, Z. Nakao, K. Miyara, Y. Nagata, and Y. W. Chen, "A new chromatic color image watermarking and its PCA-based implementation," in *ICAISC 2006, LNAI 4029*, pp. 787–795, 2006.

[18] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1069–1087, Apr. 2003

[19] M. Kutter, F. Jordan, and F. Bossen, "2Digital signature of color image using amplitude modulation," in *Storage and Retrieval for Image and Video Databases V*, I. Sethi and R. Jain, Eds. San Jose, CA: SPIE, vol. 3022, pp. 518–526, Feb. 1997.

[20] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. New York: Addison-Wesley, 1992.

