CONTENT BASED WATERMARKING FOR COLOR IMAGES USING TRANSFORM DOMAIN

S.Radharani[1], Dr. M.L. Valarmathi[2],

[1](Dept. of Comp. Applications, Sree Narayana Guru College, Coimbatore.)
[2](Dept. of Comp. Science and Engg, Govt. College of Technology, Coimbatore.)

ABSTRACT

This paper proposes three approaches to content-based watermarking for image authentication based on Independent Component Analysis (ICA). In this scheme, ICA is applied to blocks of the cover image and the resulting mixing matrix is used as the content-based feature. This is embedded in the mid-frequency DCT coefficient of the block in the first method. The watermark is embedded in the 3rd level DWT's HL3 in the second method. In the third method, DCT is computed for the third level DWT's LH3 and the watermark is embedded in the mid-frequency DCT coefficient of the block.

Index Terms –Content Based Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Fast-ICA, Frobenius Norm.

1. INTRODUCTION

A digital watermark is a technique to hide the information in a multimedia content, in such a way that it is imperceptible to a human observer which is identified by a computer. By this, the watermark is inseparable from the content.

This technique was initially used to measure the authenticity in paper and currency. In earlier days encryption is used for data protection. During data transmission, Encryption protects the content. Though, the datum is not protected after receipt and decryption. Watermarking stabilizes encryption.

Digital Watermarking has the two phases namely Watermark embedding, and Watermark extraction.

Digital watermarks can be a pseudo random sequence or a logo of a company or an image. Watermark embedding is done in the watermark carriers such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), etc of the original data resulting in watermarked data. The watermarked data may be compressed to reduce its size, corrupted by noise during its transmission through a noisy channel. It may be subjected to other normal image processing operations such as filtering, histogram modification etc.

Digital watermark technology has been developed quickly during the recent few years and widely applied to protect the copyright of digital image. A digital watermark is the information that is imperceptibly and robustly embedded in the cover data such that it cannot be removed. The watermarking procedure is to add a watermark signal to the cover data to be watermarked such that the watermark signal is unobtrusive and secure in the signal mixture.

A blind content-based watermarking scheme for authentication using ICA and DCT for grayscale images is proposed in [1]. Based on this paper, we propose color image watermarking. Watermarks are embedded in the mid-frequency DCT coefficients. DCT is a widely used technique for watermarking [2].

In [3] ICA is applied to the blocks of the cover image and the watermark image. The least-energy independent component of the cover image is replaced by the high-energy independent components of the watermark image. For watermark extraction the demixing matrices of both images are required.

In [4] treat the cover image, the key image, and the watermark image as the independent sources. Embedding is done by weighted addition of the key and the watermark to the cover image. For watermark extraction, additional two mixtures are acquired by adding the key and the watermark using different weights. ICA is then applied to these mixtures to separate the cover image, the key, and the watermark. The cover image and the key is required for watermark extraction.

ICA is used for detection of the watermark which is embedded in low frequency DCT coefficients [5].

Original DCT coefficients are required for watermark detection.

Redundant DWT (RDWT) is used in [6]. Content-based watermarking for image authentication has been worked by many authors. Paper [7] discusses a content-based watermarking scheme that uses local features of the image such as edges and zero crossings. Their scheme uses a look-up table to embed the watermark and the same table is required at the receiver end to extract the watermark. The scheme [8] embeds a Gaussian sequence watermark into low-frequency band of the wavelet transform. In their technique, watermark is embedded into visually insensitive pixels in quad-trees. A content based digital signature scheme has been presented in [9].

Choices of image features vary with techniques and directly influence the robustness of the scheme. Some techniques generate a random binary sequence to embed the watermark based on the features of the images [11]. In [12] a localization based method has been presented to verify the integrity of the received image. In these techniques the cover image is divided into several disjoint blocks and watermark is embedded in each of these blocks. To verify the authenticity of the received image, block wise authentication has been done.

In [11] image authentication has been done using content-based watermarks. But these schemes do not embed the watermark in the image content; instead embed them in the image header. These techniques distort the cover image before watermark embedding. In [13] the flippablility of a pixel is determined by connectivity preserving transition criterion.

The two vector watermarking schemes that are based on the use of complex and quaternion Fourier transforms to embed watermarks into the frequency domain that is consistent with our human visual system is proposed in [14].

2. CONTENT BASED WATERMARKING

In content-based watermarking scheme that uses local features of the image such as edges and zero crossings. Content-based watermark is generated based on salient features of the image either in spatial domains like edges, texture, and fractal dimensions etc. or in a transform domain such as singular values, Eigen values, etc. Choices of image features vary with techniques and directly influence the robustness of the scheme.

This paper aims in proposing efficient technique to provide authentication for color image. This is achieved by using Fast-ICA for generating watermark values. Techniques such as DCT, DWT, Combined DCT and DWT, are used for watermark values embedding and the same methods are used to extract the watermark values form the watermarked image.

In the scheme proposed here, the watermark generation procedure using ICA is applied to blocks of the cover image and the resulting mixing matrix represents the features of the image blocks. Frobenius norm of the mixing matrix is adapted as the content-based feature.

The Frobenius norm (FN) represents the feature of the cover image. The spatial domain and frequency-domain watermarking techniques are used to embed the watermark values in various coefficients of the blocks. This authentication technique is robust against minor image processing operations.

3. INDEPENDENT COMPONENT ANALYSIS (ICA)

A very popular method for statistical models for task learning data representations is independent component analysis (ICA), the concept of which was initially proposed by Cormon.

The ICA algorithm was initially proposed to solve the blind source separation (BSS) problem i.e., given only mixtures of a set of underlying sources, the task is to separate the mixed signals and retrieve the original sources. Neither the mixing process nor the distribution of sources is known in the process.

3.1 Fast- ICA Algorithm

One of the most popular solutions for linear ICA/ feature extraction problem is Fast ICA used to its simplicity and fast convergence. The basic algorithm involves the Preprocessing and a fixed-point iteration scheme for one unit.

3.2 Fixed-Point Iteration for One Unit

The fast ICA algorithm for one unit estimates one row of the demixing matrix W as a vector w^T, which is an extreme of contrast function. Fast ICA is an iterative fixed point algorithm, derived from a general objective or a contrast function.

Assume x is the whitened data vector and w^T is one of the rows of the rotation/ separating matrix W. Estimation of w proceeds iteratively with the following steps, until a convergence, as stated below, is achieved.

1) Choose an initial random vector w of unit norm.

2) $w \leftarrow E\{zg(w^T z)\} - Eg'(^T w)$

where $g1(y) = y^3$ (derivative of kurtosis),

$g2(y) = \tanh(ay)$, $1 \le a \le 2$

and g'(y) are the corresponding derivatives.

3) $w \leftarrow w / \| w \|$ where $\|w\|$ is the norm of w.

4) If $w_{old} - w_{new} \leq \varepsilon$ is not satisfied, then go back to step 2,

where ε is a convergence parameter and w_{old} is the value of w before its replacement by the newly calculated value w_{new}.

4. PROPOSED METHOD

To achieve authentication for color images the proposed scheme make use of the following the three phases

i. Watermark generation
ii. Watermark embedding
iii. Watermark extraction and authentication

4.1 Watermark Generation Using Fast-ICA

The following procedure is used to generate the watermark values for all the watermark techniques.

1. Segment the watermark image I of size n x n into blocks of size m x m resulting in K blocks.
2. Perform ICA of each block treating each row of the block as a vector.
3. Extract the mixing matrix A.
4. Compute the Frobenius norm of the mixing matrix; this is the content-based watermark w of the block.
5. Repeat steps 2 – 4 for computing the watermark for all the blocks. This set forms the watermark,

W= $\{w_1, w2, \ldots, wk\}$

4.2 Watermark Embedding

4.2.1 Discrete Cosine Transform (DCT)

1. Compute DCT of each block of cover image.
2. Select the mid-frequency coefficient at the chosen location (p, q) in each block.
3. Replace the chosen coefficient with the watermark:

   DCT (p, q) =sign (DCT (p, q))* (α*w)

   where α- embedding strength
4. Perform inverse DCT.
5. Repeat steps 1– 4 for all the blocks. The resultant is the watermarked image I*.

4.2.2 Discrete Wavelet Transform (DWT)

1. Apply DWT (Haar wavelet) to decompose the cover image into four non-overlapping multi-resolution sub-bands:LL_1, HL_1, LH_1 , HH_1. Similarly apply two times to get the 3rd level sub-bands: LL_3, HL_3, LH_3, HH_3.
2. To replace mid component with scaled watermark wit same sign

   HL_3 = (sign (HL3))* α *w (k)

   where α- embedding strength
3. Perform inverse DWT.
4. Repeat steps 1 & 2 for all the blocks. The resultant is the watermarked image I*.

4.2.3 Combined DCT and DWT

1. Apply DWT (Haar wavelet) to decompose the cover image into four non-overlapping multi-resolution sub-bands:LL_1, HL_1, LH_1, HH_1. Similarly apply two times to get the 3rd level sub-bands: LL_3, HL_3, LH_3, HH_3.
2. Compute DCT of sub band LH_3.
3. To replace mid component with scaled watermark wit same sign

   DCT (p, q) = (sign (DCT (p, q)))* α *w (k)

   where α- embedding strength
4. Perform inverse DCT and DWT.
5. Repeat steps 1– 2 for all the blocks. The resultant is the watermarked image I*.

4.3 Watermark Extraction and Authentication

4.3.1 Discrete Cosine Transform (DCT)

1. Perform steps 1–5 of the watermark generation procedure on the received image and obtain the computed watermark.
2. Compute DCT of each block.
3. Extract the embedded watermark from the chosen DCT coefficient:

   W'=|DCT (p, q)|/α

   where α- embedding strength
4. This set forms the extracted watermark.

   W'= $\{w'_1, w'_2, \ldots, w'_k\}$
5. Calculate the block wise percentage difference (Δ) between the watermark values w* and w':

   $\Delta = (|W_i^* - W_i| * 100 * 0.2) / \max\{W_i^*\}$

4.3.2 Discrete Wavelet Transform (DWT)

1. Perform steps 1–5 of the watermark generation procedure on the received image and obtain the computed watermark.
2. Compute DWT of cover image.
3. Extract the embedded watermark from the chosen DWT sub band

   W'=$|HL_3|$/α

   where α- embedding strength
4. This set forms the extracted watermark.

   W'= $\{w'_1, w'_2, \ldots, w'_k\}$
5. Calculate the block wise percentage difference (Δ) between the watermark values w* and w':

   $\Delta = (|W_i^* - W_i| * 100 * 0.2) / \max\{W_i^*\}$

4.3.3 Combined DCT and DWT

1. Perform steps 1–5 of the watermark generation procedure on the received image and obtain the computed watermark.
2. Compute DWT of cover image.

3. Compute DCT of Sub band HL_3.
4. Extract the embedded watermark from the chosen DWT sub band
   W'=|DCT (p, q)|/α
   where α- embedding strength
5. This set forms the extracted watermark.

W'= $\{w'_1, w'_2, \ldots, w'_k\}$

6. Calculate the block wise percentage difference (Δ) between the watermark values w* and w':
   $\Delta = (|W_i^* - W_i| * 100 * 0.2) / \max\{W_i^*\}$

4.4 Choice of Parameters

4.4.1 Block Size

Choosing a block size is based on the processing time and relevant features. Blocks of small size leads to poor performance in watermarking process and larger blocks demand high computational time. Hence a trade off among these two is required to choose the block size. After experimentation, a block size of 16 x 16 was chosen as it resulted in better PSNR value, computational time and better feature representation.

4.4.2 Embedding Location

To embed the watermark in a suitable location the proposed technique uses one of the mid frequency coefficient, because low-frequency components degrade the cover image. Similarly high-frequency components are not advisable as they may be lost during compression. Therefore the watermark is embedded in mid-frequency components to ensure robustness. The mid-frequency coefficient to embed the watermark is chosen as the mid-diagonal coefficient i.e., the location (block size/2, block size/2).

4.4.3 Embedding Strength (α)

For choosing a suitable value for the embedding strength (α), statistics of the DCT coefficient values at that mid-diagonal location of all the blocks are obtained, specifically the standard deviation α_x .Similarly the standard deviation α_w is obtained for the watermark. The value of embedding factor α is determined such that the watermark values are suitably scaled to have the same range of variation as that of the DCT coefficients.

$$\alpha = \alpha_x / \alpha_w$$

In this after experimentation the value of α is assumed as 0.14.

4.4.4 Threshold

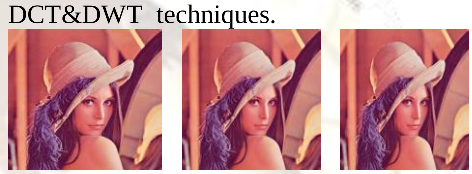
Threshold for the percentage difference Δ between the watermarks have been experimentally determined as 15%. Thresholds less than 15% resulted in false negatives; while higher than 15% thresholds made the technique to be fragile.

5. RESULTS AND SNAPSHOTS

The original color images are shown in the Figure 1.

Fig.1 The Original Color Images

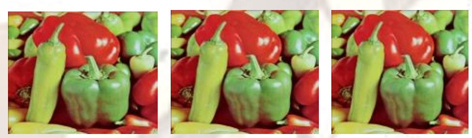
Figure 2 (a-c) shows the watermarked images obtained by embedding the watermark values with the images using DCT, DWT, Combined DCT&DWT techniques.



(a) (b) (c)

Fig.2 Color Images after Watermarking using Fast-ICA.

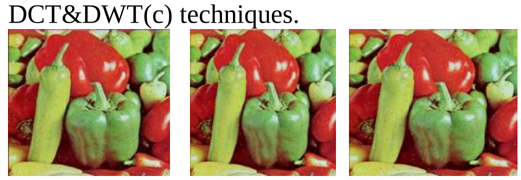
Figure 3 (a-c) shows the watermarked color images after applying JPEG Compression obtained by embedding the watermark values with the images using DCT, DWT, Combined DCT&DWT techniques.



(a) (b) (c)

Fig.3 Effect of watermarked Images after JPEG Compression Attack.

Figure 4 (a-c) shows the watermarked color images after applying white noise obtained by embedding the watermark values(Frobenius norm) with the images using DCT(a), DWT(b), Combined DCT&DWT(c) techniques.



(a) (b) (c)

Fig.4 Effect of watermarked Images after White Noise Attack.

5.1 Extraction Efficiency

The efficiency of the scheme in correctly extracting the watermark is given by the percentage difference among the computed and extracted Frobenius norm of the mixing matrix of the received image blocks. Table.1 gives the highest percentage difference Δ for some various watermarking techniques for the test images. The values are small, range from 1.2127 to 6.3657, over all the test images for various watermarking techniques using ICA. This shows that the scheme extracts the embedded watermark accurately.

TABLE.1
RESULTS AFTER WATERMARK EXTRACTION WITHOUT ATTACKS

S. NO	IMAGE NAME	HIGHEST PERCENTAGE DIFFERENCE		
		DCT	DWT	Combined DCT and DWT
1	LENA	2.563	2.475	2.475
2	SAILBOAT	5.715	3.822	6.365
3	PEPPER	3.772	2.517	2.517
4	BABOON	3.467	4.869	4.315
5	JETPLANE		2.707	2.7072
6	HOUSE	1.212	3.320	3.320
7	GRILS	3.428	5.216	3.596
	AVERAGE	3.197	3.561	3.614
	MINIMUM	1.212	2.475	2.475
	MAXIMUM	5.715	5.216	6.365

From the Figure 5 DCT method produces better results than other two techniques.

5.2 Quality of the Watermarked Image

The proposed content-based watermarking scheme has been carried out on a set of images of three categories. The metrics PSNR, Pearson Correlation Coefficient (PCC), Normalized Cross Correlation (NCC), and Image Fidelity (IF) are calculated between the cover image and the watermarked image for various watermarking techniques. It can be observed that there is no perceptually noticeable difference in the images due to watermarking.

In Table.2 the quality metrics of the watermarked images using Frobenius norm as the feature of different methods are compared.

TABLE 2.
QUALITY METRICS AFTER WATERMARKING

EMBEDDING METHODS	PARAMETER	IMAGE NAME									
		LENA	SAIL BOAT	PEPPER	BABOON	JETPLANE	HOUSE	GIRLS	AVERAGE	MINIMUM	MAXIMUM
COMBINED	PCC	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	IF	1.000	0.999	1.000	0.999	1.000	0.999	1.000	0.999	0.999	1.000
	NCC	1.000	1.000	1.000	0.999	1.000	1.000	1.000	0.999	0.999	1.000
	PSNR	78.335	79.114	79.376	76.776	79.147	80.563	79.147	78.929	76.776	80.563
DWT	PCC	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	IF	1.000	0.999	1.000	0.999	1.000	0.999	1.000	0.999	0.999	1.000
	NCC	1.000	1.000	1.000	0.999	1.000	1.000	1.000	0.999	0.999	1.000
	PSNR	78.335	79.111	79.372	76.776	79.149	80.563	79.149	78.922	76.77	80.563
DCT	PCC	1.000	1.000	0.999	1.000	1.000	1.000	1.000	0.999	0.999	1.000
	IF	1.000	1.000	1.000	0.999	1.000	1.000	1.000	0.999	0.999	1.000
	NCC	0.999	0.999	0.999	0.999	0.999	0.999	1.000	0.999	0.999	1.000
	PSNR	78.646	79.089	79.401	76.702	78.375	80.587	79.712	78.930	76.703	80.587

ATTACKS	PARAMETERS	HIGHEST PERCENTAGE DIFFERENCE		
		DCT	DWT	Combined DCT &DWT
JPEG Compression	Compression Ratio			
Maximum	100	8.441	15.600	15.543
High	80	8.974	15.600	15.321
Medium	60	12.721	14.492	14.324
Low	40	11.471	15.600	15.453
Noise				
Uniform	Percent=5	14.724	17.526	19.540
Gaussian	Mean=1 Variance=0.01	15.344	18.405	17.600
Filter				
Low pass	Standard Deviation = 10	11.892	18.682	17.453
Sharpening	-	15.486	16.783	16.231
Gamma Correction		7.467	7.674	7.654
AVERAGE		11.836	15.596	15.457
MINIMUM		7.467	7.674	7.654
MAXIMUM		15.486	18.682	19.540

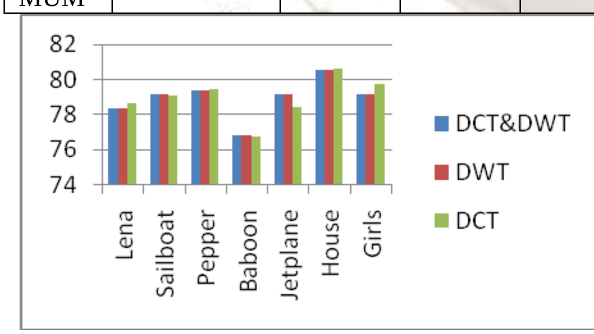


Fig. 5 PSNR of Various Images under various Transform domains.

5.3 Robustness against Incidental Image Processing

Robustness of the proposed scheme against normal signal processing operations such as jpeg compression, noise and filtering has been experimentally evaluated on all the test images.

For all the attacks, the values of highest percentage difference Δ using ICA, ranges from 7.4670 to 19.5402 for various watermarking techniques as given in Table 3.

TABLE.3
RESULTS AFTER INCIDENTAL DISTORTIONS ON COLOR IMAGES

In this proposed watermarking technique the watermarked image is subjected to two types of distortions noise and filter. The noise added to the watermarked image is Gaussian noise and uniform noise. Also filtering such as contrast stretching has been applied on the watermarked image.

From Fig. 6, DCT technique shows the good performance of robustness after attacks comparing to other two techniques for the test images.

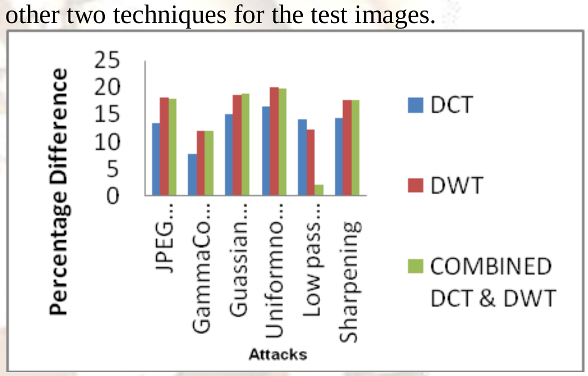


Fig. 6 Robustness of Fast-ICA after attacks

6. CONCLUSION

In this paper various content based watermarking techniques are carried out. Here the content of images is Frobenius norm which is obtained using Fast-ICA method. No information about the cover image is required for watermark extraction. For watermark embedding, three techniques such as DCT, DWT, Combined DCT and DWT are used. The same methods are used to extract the watermark values successfully and the results are compared. The proposed methods correctly authenticate the images even under normal image processing operations. The comparison of three transformed techniques shows that DCT based watermarking application provides better result.

In addition to this various attacks are applied on the watermarked images. Robustness of the proposed scheme against normal signal processing operations such as jpeg compression, noise and filtering has been experimentally evaluated on all the test images.

REFERENCES

[1] Dr. Latha Parameswaran, Dr. K. Anbumani, Content-Based Watermarking for Image Authentication Using Independent Component Analysis, Informatica 32 (2008), 299-306.

[2] Francisco J. Gonzalez-Serrano, Harold. Y. Molina-Bulla, and Juan J. Murillo-Fuentes, May 2001, Independent component analysis applied to digital image Watermarking, International Conference on Acoustic, Speech and Signal Processing (ICASSP), vol. 3, 1997-2000.

[3] Dan Yu, Farook Sattar, and Kai-Kuang Ma, 2002, Watermark detection and extraction using independent component analysis method, EURASIP Journal on Applied Signal Processing, vol. 1, 92–104.

[4] Minfen Shen, Xinjung Zhang, and Lisha Sun, P. J. Beadle, F. H. Y. Chan, April 2003, A Method for digital image watermarking using ICA, 4th International Symposium on Independent Component Analysis and Blind Signal separation (ICA 2003), Nara, Japan, pp. 209-214.

[5] Ju Liu, Xingang Zhang, Jiande Sun, and Miguel Angel Lagunas, April 2003, A Digital watermarking scheme based on ICA detection, 4th International Symposium on Independent Component Analysis and Blind Signal Separation, (ICA 2003), Nara, Japan, 215-220.

[6] Stephane Bounkong , Boremi Toch , David Saad , and David Lowe , 2003 , ICA for watermarking digital images, Journal of Machine Learning Research 4, 1471-1498.

[7] Chang-T sun Li, Der Chyuan Lou, and Tsung_Hsu Chen, Image authentication and integrity verification via content-based watermarks and a public key cryptosystem, Proceedings of International Conference on Image Processing, vol. 3, 2000 694-697.

[8] . Kil-Sang Yoo, Mi-Ae Kim, and Won-Hyung Lee, A robust image watermarking technique for JPEG images using quad trees, Lecture Notes in Computer Science, vol. 3332, 34-41, 2004.

[9] Marc Schneider and Shih-Fu Chang, September 1996, A robust content based digital signature for image authentication, Proceedings of International Conference on Image Processing, vol. 3, 227-230.

[10] Chai Wah Wu, September 2002, On the design of content-based multimedia Authentication systems, IEEE Transactions on Multimedia, vol. 4, no.3, 385- 393.

[11] Eugene T. Lina, Christine I. Podilchuk, and Edward J. Delp, January 2000, Detection of Image alterations using semi - fragile watermarks, Proceedings of SPIE International Conference on Security and watermarking of Multimedia contents.

[12] Phen-Lan Lin, Po-Whei Huang, and An-Wei Peng, 2004, A fragile watermarking scheme for image authentication with localization and recovery, Proceedings of the IEEE Sixth International Symposium on Multimedia Software Engineering (ISMSE'04).

[13] Huijuan Yang and Alex C. Kot, December 2006. Binary image authentication with tampering localization by embedding cryptographic signature and block identifier, IEEE Signal Processing Letters, vol. 13, no. 12, 741-744.

[14] Tsz Kin Tsui, Xiao-Ping Zhang Androutsos, Color Image Watermarking Using Multidimensional Fourier Transforms, IEEE Transactions on Information Forensics and security, Vol. 3, 16-28, March 2008.