Reversible Blind HF Domain Contourlet Watermarking for Authentication of Digital Images

R.Velumani
Associate Professor & Head
Department of IT
Sethu Institute of Technology
Pulloor, Kariapatti, India - 626115.

V.Seenivasagam
Professor & Head
Department of CSE
National Engineering College
Kovilpatti, India - 628503.

ABSTRACT

Digital images are widely used in defense, e-governance, medicine, banking, insurance, healthcare, scientific research, weather forecasting etc. Varied applications in these fields demand the secure exchange of digital images that serve as valid document evidences for legal procedures and for clinical, scientific and forensic analysis. These images are susceptible to intentional or accidental attacks during transit which may lead to the loss of confidentiality and integrity of the content and identity of the sender. This paper presents a reversible blind watermarking scheme for authentication of digital images with a binary logo. It exploits the contourlet domain for watermarking as it preserves the smooth contours and edges even after multiple levels of decomposition. The proposed watermarking algorithm embeds the watermark in an arbitrary sparse High Frequency (HF) subband; the watermark extraction algorithm follows a unique hard thresholding approach for blind watermark extraction. The system applies a triangular number generating function to strengthen the binary watermark and employs Arnold transform for watermark synchronization. Experimental results show that the proposed system provides good fidelity of watermarked and recovered images and robustness to certain geometrical and non geometrical attacks.

Keywords

Authentication, blind watermarking, reversible watermarking, triangular number, Arnold transform

1. INTRODUCTION

With significant growth in multimedia and networking, valid documents in the form of digital images are exchanged over the WWW. These images are prone to intentional and accidental attacks on the fly. Hence they must be protected against attacks and their ownership must be established in case of disputes. Further, the advent of services such as telemedicine, teleradiology, telesurgery, and remote patient monitoring etc., have led to the digitization of the patient information, medical history and clinical images. These images may be tampered on transit leading loss of identity, integrity, confidentiality and authenticity. This paper presents a watermarking system for authentication of digital images with a binary logo focusing on the aspects of blind watermarking and reversibility.

Reversibility is an essential feature to be imbibed in any watermarking system designed for the authentication of images that contain significant features, the loss of which cannot be compromised. Higher the degree of reversibility achieved, higher is the intactness of the cover image and lower is the loss of details. This technique has gained significance as many of the critical applications such as forensics, telemedicine, and copyright protection etc., demand the lossless reconstruction of the cover image. Many reversible watermarking schemes have been proposed by various researchers in various domains starting with the application of modulo addition for an additive[1] watermark, the use of losslessly compressed bit-planes[2] in the spatial domain followed by a technique in which watermarking is done by exploiting the redundancy[3] characteristics of the neighboring pixels and a multiplicative method proposed by Li et al[4] to embed the watermark composed of pseudo-random sequence with the selected Contourlet Transform coefficients modeled with Generalized Gaussian Distribution with zero mean.

Blind extraction refers to the extraction of the watermark from the watermarked image without the need for the original image at the receiver's end. This feature thwarts the risk of exchange of the cover image and hence protects it from being copied and distributed in unauthorized ways. It is a promising scheme that has invited attention of the researchers in the recent years. Blind watermarking when combined with reversible steganography improves the strength of the watermarking system. As watermarking in the spatial domain leads to visual degradation, easy detection and destruction of watermarks, the cover images are subjected to multi resolution transforms and watermarks are embedded in suitable subbands. Since the proposal of the Contourlet Transform by Do and Vetterli[5], many watermarking schemes have been proposed exploiting the characteristics of the contourlet subbands.

Our paper proposes a scheme for reversible blind watermarking in HF coefficients of the contourlet subbands. It employs the concept of triangular[6] numbers for reversibility, Arnold Transform[7] for watermark synchronization and a hard thresholding approach for blind extraction of the watermark. The paper is organized with an introduction to the contourlet domain watermarking in section 2, followed by a discussion on Arnold transforms in section 3 and image quality and performance metrics in section 4. The proposed system is discussed in section 5 and experimental results are given in section 6. A discussion on the results is given in section 7, the paper is concluded in section 8 and references are listed in section 9.

2. CONTOURLET DOMAIN WATERMARKING

The Contourlet Transform proposed by Do and Vetterli is an extension of the wavelet transform. It is obtained by combining both Laplacian Pyramid (LP) and Directional Filter Bank (DFB). The transform is implemented with a filter bank that decomposes an image into several directional subbands at multiple scales. This transform effectively captures the smooth contours and edges of the image subjected to decomposition. The contourlet decomposition and directional partitions are illustrated in Figure 1 and Figure 2 respectively.

Contourlet Transforms are used in various image processing applications like fusion, registration, de-noising, face detection etc,. Significant research has been carried out regarding watermarking in the contourlet domain and different approaches have been proposed exploiting the statistical[8] features of the contourlet coefficients.

Given an image I, at each level j of contourlet decomposition, a lowpass image I_j is being generated at the LP stage and a set of band pass images B_j, $j=1,2,...2^k$, where k is the number of directional decompositions at each level are generated at the DFB stage. While the lowpass image preserves the low frequency components, high frequency components are being preserved by the directional subbands. The above process may be repeated for the desired level of decomposition by iteratively feeding the lowpass image to the LP stage and so on.

Generally, all the methodologies for watermarking in the contourlet domain follow an additive approach to embed a watermark in a highest energy subband. Given $I(x,y)$, the intensity of the subband of size nxn , its energy is calculated as in (1).

$$E = \sum_{x=1}^{n} \sum_{y=1}^{n} \left| I(x,\ y) \right|^2 \qquad (1)$$

A selected contourlet coefficient is modified as in (2) to carry an element of the watermark which can be retrieved later.

$$C_i = c_i + \propto w_i \qquad (2)$$

where

c_i is the candidate coefficient
w_i is the watermark image coefficient
α is the strength factor
C_i is the watermarked coefficient

The extraction process is performed by applying the Inverse Contourlet Transform on the watermarked image and suitable mathematical operations in the selected subbands. The above approach is followed in the schemes proposed by Li et al. and S.M.E.Sahraeian et al[9], in which , the subband energy is computed in the selected scale and the one with more energy is selected as the candidate band for embedding in order to protect the perpetually significant features as proposed by Cox et al[10]. Similarly Song et al[11] proposed a scheme in which the HF subbands are chosen for watermarking as they are robust to HF image processing.
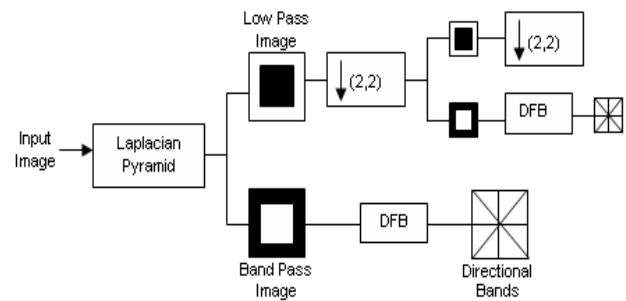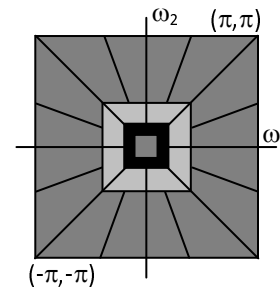

Fig1: Contourlet Decomposition

Fig 2: Directional Partition

Elham Salahi et al[12] presented a scheme in which two subbands with highest and lowest variance in the finest scale are selected for embedding, as they contain the high frequency components of the cover image which provide high imperceptibility and robustness. Shereen et al[13] presented an algorithm in which the watermark is embedded into the visually insensitive coefficients in the lowest frequency band and their cousins and children in other bands and levels.

Our paper presents an approach for embedding a binary logo in the arbitrary coefficients of arbitrary HF contourlet subbands irrespective of their energy, exploiting their sparseness. The sparse nature of the contourlet coefficients can be evidenced from the representation of the subbands in section 6.

3. ARNOLD TRANSFORMS

Chaotic transforms are commonly applied for scrambling the watermarks before embedding them into the host images. Applying a chaotic function recursively on a watermark will render it unintelligible and it cannot be deciphered correctly unless the number of iterations and initial conditions are known by the attacker. The commonly used transforms for scrambling are Gray Code, Fass Curve, Arnold Transform, Magic square etc. Any image scrambled with the Arnold Transform comes back to its original form after certain number of iterations. This feature is exploited in the watermarking algorithms to improve the security of the watermarks. The application of different chaotic maps for digital watermarking has been elaborately discussed by Athanasios and Pitas[14]. Their paper concludes that the watermarks scrambled with N-way tailed shift function are robust and those scrambled with Renyi map are less resistant to attacks. A watermarking algorithm proposed by Xianyong

Wu et al[15], employs the Arnold map to encrypt the embedding position of the host image and the logistic map to determine the bit positions for embedding. The Arnold transform is given in (3).

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\ n) \qquad (3)$$

Any coordinate position (x,y) can be mapped to (x_n,y_n) within an nxn space by applying (3) for the required number of iterations. Similarly (x_n,y_n) can be transformed back to (x,y) applying (3) for the same number of iterations. Synchronization, i.e., locating the positions of the watermarked coefficients is essential for watermark extraction. This issue has been addressed in many literatures and many synchronization schemes have been proposed. Feature point based synchronization with a Harris interest point and other detectors and embedding in the invariant regions of images have been discussed by Lei-Da Li et al[16]. Though perfect synchronization can be accomplished with a mapping table that records the embedding positions, the use of this table for watermark extraction renders the system to be non blind. However, the chaotic and invertible nature of the Arnold Transform, makes it suitable for both watermark scrambling and synchronization.

4. IMAGE QUALITY AND PERFORMANCE MEASURES

The performance of the watermarking systems can be evaluated by computing various discrete image quality measures on the watermarked images. The various metrics used to determine the closeness of the processed and the original images are discussed in this section. The common metrics used in various image compression and watermarking systems are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). The smaller value of MSE is an indication of good quality of the processed image while a higher value of MSE signifies poor image quality. PSNR is a measure of the image fidelity i.e., a measure of the distortion. A small value of PSNR is an indication of low imperceptibility while a large value indicates a good degree of imperceptibility.

The Structural Similarity Index Measure (SSIM) is used to evaluate the quality of a processed imaged based on its structural similarity with the unaltered image as the reference. Recently, the Universal Image Quality Index (UIQI)[17] measure that takes into account of structural distortions is used as a replacement for MSE and PSNR measures. Our system also uses the Weighted PSNR (WPSNR) and Mean Structural Similarity Index Measure (MSSIM) metrics to evaluate the perceptual image quality. Further, it evaluates the robustness of the watermark with the Normalized Mean Square Error (NMSE) measure.

Since this paper focuses on reversibility, it is required to ensure that the reconstructed cover images contain less distortions i.e., their fidelity is preserved. Hence, the same metrics discussed above are used to measure the imperceptibility of the watermarked images and the fidelity of the recovered cover images with the original cover images as reference.

5. PROPOSED SYSTEM

In this section the embedding and extraction algorithms are discussed in subsections 5.1 and 5.2 respectively. Unlike the algorithms for HF band watermarking proposed in the earlier literatures which select the subband with the highest energy, this algorithm selects an arbitrary subband to prevent an intruder from attacking the highest energy subband. It also selects the arbitrary coefficients based on Arnold map to hide the watermark. The proposed system applies the concept of a triangular number generating function that uniquely encodes a pair of positive integers into a positive integer as in (4). The pattern of triangular numbers is shown in Figure 3. Table 1 shows the coded representation of different integer pairs using (4). The first row of the table contains triangular numbers in sequence shown in red bold faces.
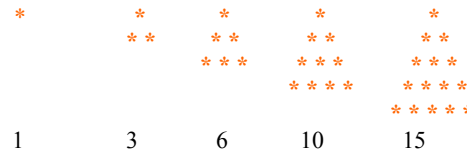
$$T = f(a,b) = [(a + b)^2 + 3a + b]/2 \qquad (4)$$

Fig 3: Triangular numbers

Table1. Integer Pair Representation

b／a	0	1	2	3
0	**0**	**1**	**3**	**6**
1	2	4	7	11
2	5	8	12	17
3	9	13	18	24

On applying the steps for extraction from (5) to (7), any number in the table, *T* can be factored into *a* and *b* exactly, irrespective of the triangular nature, without any additional information. Hence it serves as the best approach for imbibing reversibility.

$$C = [\mathrm{sqrt}(8T + 1) - 1]/2 \qquad (5)$$
$$\text{where } C = a + b$$

$$a = T - C(C + 1)/2 \qquad (6)$$

$$b = C(C + 3)/2 - T \qquad (7)$$

The Arnold transform is applied to select the embedding position in the candidate subband. For the watermark of size NxN, the coordinate position (x,y) of the watermark is mapped to (x_n,y_n) of the candidate subband. This transform not only scrambles the watermark, but also aids in watermark synchronization during extraction.

5.1. *Watermark Embedding*

The algorithm followed for watermark embedding is as follows.

1. Apply Contourlet Transform to the selected cover image and generate the subbands selecting *s*, the desired scale for decomposition and *n*, the number of directional decompositions at each scale.
2. Select an arbitrary HF subband as the candidate subband *C* for embedding
3. Choose the initial conditions for Arnold Transform
   a. Initial pixel position *(i,j)*
   b. Number of iterations *k*
4. Map the position *(i,j)* of watermark bit w_{ij} in the watermark to (i_n, j_n) of the candidate subband in *k* iterations . Let C_{ij} be the candidate coefficient.
5. If watermark bit w_{ij} is 0, do not alter C_{ij}; Else, generate the watermarked coefficient as $C_{ij} = f(const, w_{ij})$ where *const* is a scalar constant.
6. Repeat steps 4 and 5 for all the bits in the watermark
7. Apply inverse Contourlet Transform on all the subbands to generate the watermarked image

Equation (4) can be applied over every individual pair of the candidate coefficient and the watermark bit to generate the watermarked coefficient. However, in this system, as the candidate coefficients are negative in nature, (4) cannot be applied directly over them. Hence the function is applied on a positive constant *const* and the watermark bit w_{ij} as in (8).

$$C_{ij} = f(const, w_{ij}) = [(const + w_{ij})^2 + 3 * const + w_{ij}]/2 \quad (8)$$

The watermarked coefficients are susceptible to significant degradation as they are influenced by the parents, neighbors and cousins due to interdependencies as discussed in a paper by Rabbani et al[18]. The value of *const* is chosen in such a way that the positive nature of C_{ij} is preserved.

5.2 *Watermark Extraction*

The watermark extraction algorithm is as follows.

1. Apply inverse Contourlet Transform on the watermarked image based on *s* and *n*
2. Choose the arbitrary watermarked HF subband
3. Apply Arnold Transform using initial conditions to get the positions (i_n, j_n) of the watermarked coefficients C_{ij}
4. Determine the watermark bit by hard thresholding
   a. Check the sign of C_{ij}
   b. If $C_{ij} > 0$ assign watermark bit $w_{ij} = 1$
   c. Else assign $w_{ij} = 0$
5. If C_{ij} is positive, replace each watermarked coefficient C_{ij} with the smallest of the coefficients in the watermarked HF subband
6. Repeat steps 4 and 5 for all the bits in the watermark
7. Generate the watermark image out of the individual bits w_{ij}
8. Apply Contourlet Transform on LF and HF bands to recover the cover image

and w_{ij}. However, as the value of *const* is unique, as it is not

significant for reconstruction and due to the complexity of the factoring algorithm, only sign checking is performed on the watermarked coefficients as identified by the Arnold Transform to determine the value of w_{ij}.

6. EXPERIMENTAL RESULTS AND COMPARISONS

The proposed system has been implemented and tested in Matlab7.0. The 512x512 sized standard *Baboon*, *Barbara*, *Lena* and *Peppers* images are chosen as cover images. These images are given in Figure 4(a) to 4(d). A binary logo and a image pattern each of size 32x32 and 64x64, chosen as watermarks are as shown in Figure 5(a) and 5(b) respectively. Each of the watermarks is embedded in each of the cover image and the performance metrics are evaluated and tabulated in this section. The resultant images are shown for both embedding and extraction of the 32x32 and 64x64 watermarks with the *Baboon and Peppers* images respectively. The value of *const* used in the embedding algorithm is chosen to be 5.

Fig 4: (a) *Baboon* (b) *Barbara* (c) *Lena* (d) *Peppers*
Cover Images

Fig 5:(a) 32x32 logo (b) 64x64 Image pattern
Watermark Images

To begin with, the cover image is decomposed by Contourlet Transform to 3 scales to generate the low pass subband and high frequency directional subbands. The number of directional subbands is 8, 16 and 4 starting from the coarsest to finest level of decomposition in the high frequency bands. The *9-7* and *pkva* filters are chosen for LP and DFB stages respectively. The contourlet subbands of *Baboon* and *Peppers* images are shown in Figure 6(a) and 6(b) respectively.

Out of all the generated subbands, 16 subbands in the third level of decomposition, have been chosen for embedding the 32x32 logo as each subband is comparatively larger than the watermark. Invariably, the watermark is embedded with the same algorithm in each subband of the 3rd level in sequence. Similarly, for the 64x64 image pattern, the finest scale that contains 4 subbands each of size 256x256 is chosen for embedding. The watermarked images generated with the embedding schemes are shown in Figure 7(a) and 7(b).
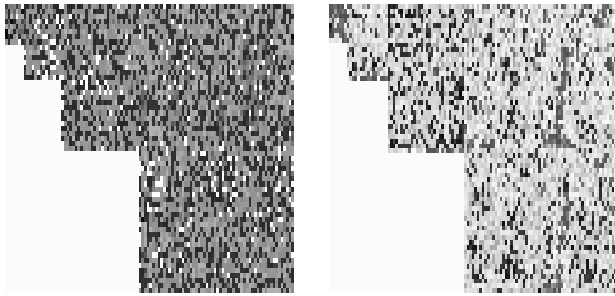
Fig 6: Contourlet Subbands (a) *Baboon*   (b)*Peppers*

Fig 7: Watermarked Images (a) *Baboon*   (b) *Peppers*

The 32x32 watermarks extracted from the 16 subbands of the watermarked *Baboon* image are given in Figure8(a); similarly and 64x64 watermarks extracted from the 4 subbands of the *Peppers* image are shown in Figure 8(b).
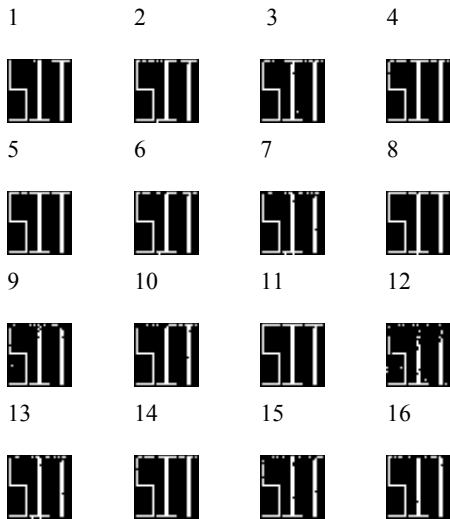

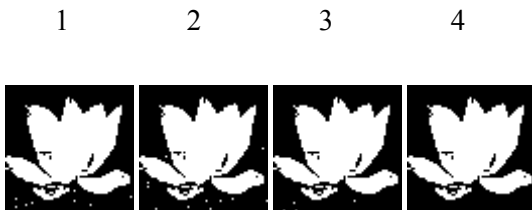**Fig 8:(a) Watermarks Extracted from *Baboon***

Fig 8:(b) Watermarks Extracted from *Peppers*

The performance of the embedding algorithm has been evaluated with various quality measures discussed in section 4. The various metrics are computed with the original images as reference images in order to evaluate the imperceptibility. The mean of the performance metrics comparing the original images and the watermarked images are shown in the Table 2. From the values of the SSIM and UIQI measures listed in Table 2, it is evident that the watermarked images possess a high degree of imperceptibility. Further it is also seen that PSNR values are as high as 35dB for both 32x32 and 64x64 logos, which is an indication of good image fidelity. It is seen that values of SSIM and UIQI are very close to 1, clearly indicating that the watermarked images do not contain any obvious visual artifacts leading to degradation i.e., their imperceptibility is good.

Table 2. Mean of Performance Metrics for Watermarked Images

Host Image Metric		Baboon	Barbara	Lena	Peppers
PSNR in dB	32x32	43.5912	45.5196	47.4927	47.5253
	64x64	35.5645	36.8906	40.0407	39.8771
WPSNR in dB	32x32	55.7048	57.7725	59.6915	59.7492
	64x64	48.9677	50.366	53.4401	53.2286
MSSIM	32x32	0.9987	0.9985	0.9984	0.9984
	64x64	0.9995	0.9994	0.9991	0.9988
SSIM	32x32	0.9978	0.9977	0.9976	0.9975
	64x64	0.998	0.9973	0.998	0.9975
UIQI	32x32	1	1	1	0.9998
	64x64	1	1	1	0.9991

Reversibility of the watermarking system can be evaluated by computing various image fidelity metrics on the recovered cover images with the original images as the reference. The mean of the performance metrics comparing the original image and the recovered images are listed in Table 3.

Table 3. Mean of Performance Metrics for Recovered Images

Host Image Metric		Baboon	Barbara	Lena	Peppers
PSNR in dB	32x32	42.7392	42.2228	45.33	46.3739
	64x64	37.259	37.2752	42.5699	39.8269
WPSNR in dB	32x32	54.8213	54.3953	57.6448	58.788
	64x64	50.6638	50.6709	56.0041	53.2085
MSSIM	32x32	0.9978	0.9947	0.9954	0.9949
	64x64	0.9995	0.9993	0.9993	0.9985
SSIM	32x32	0.9962	0.9915	0.9925	0.9914
	64x64	0.9974	0.9966	0.9982	0.9955
UIQI	32x32	1	1	1	0.9996
	64x64	1	1	1	1

From the above tables it is seen that the fidelity and structural aspects of the cover image are preserved after dewatermarking both 32x32 and 64x64 watermarks. The performance of the proposed scheme is compared with the earlier methods with respect to the PSNR values computed between the original and the watermarked images. Since watermarking is performed in all the subbands of the selected scale in this method, the mean PSNR value obtained in a scale is taken for comparison with that obtained from other methods. Further, as different images are chosen in different papers, comparison statistics are given wherever appropriate. The comparison of PSNR values is given in Table 4. Also, the proposed method provides a better PSNR for *Lena* image compared to 40.84dB that is obtained from the method proposed by Jayalakshmi et al[19] and for *Baboon* and *Barbara* images against the values 39.53dB and 36.63dB obtained with the method proposed by Sahraeian et al.

Table 4. PSNR Values of Watermarked Images in dB

Method \ Host Image		Baboon	Barbara	Lena	Peppers
Proposed System	32x32	**43.5912**	**45.5196**	**47.4927**	**47.5253**
	64x64	**37.7193**	**38.7371**	**42.5941**	**41.765**
Shereen et al.		41.2653	Not Used	41.2612	41.2780
H.Song et al.		Not Used	35.25	36.65	34.98
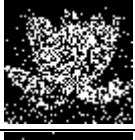
Table 5 contains the comparison between the proposed method and the algorithm proposed by Shereen et al. that embeds the bits in both the LF and HF contourlet subbands for the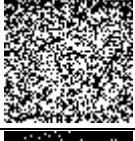 WPSNR and MSSIM metrics. The metrics shown in bold faces correspond to the proposed method. It is seen that the proposed method offers better fidelity compared to the highly complex algorithm in which both the low and high frequency subband coefficients are chosen for watermarking.

Table 5. Proposed Vs LF & HF Embedding

Metric \ Host Image	Baboon	Lena	Peppers
WPSNR in dB	**55.7048**	**59.6915**	**59.7492**
	45.2170	42.1866	42.3675
MSSIM	**0.9987**	**0.9984**	**0.9984**
	0.9868	0.9652	0.9667

The watermarked images are generally vulnerable to intentional and accidental attacks during transmission. The robustness of the proposed system has been tested with various geometric and non geometric attacks. The watermarked images are subjected to various attacks using Checkmark[20] software and the watermark extraction algorithm has been applied to the distorted images. The attacks on the watermarked *Baboon* and *Peppers* images and the extracted watermarks with corresponding NMSE values are listed in Table 6.

Table 6. Attacks and Extracted Watermarks

Attack	Watermark Extracted 32x32	NMSE	Watermark Extracted 64x64	NMSE
Cropping		2.5682		2.0556
Gaussian		0.0126		0.1031
Hard Thresholding		0.854		0.6645
JPEG Compression (50%)		0.8791		0.9647
Sampling		0.0502		1.1208
Scaling (50%)		0.4772		1.4881
Shearing (50%)		3.2338		2.0546
Soft Thresholding		0.8477		1.0288
Template Removal		0.6844		0.9097
Wavelet Compression (50%)		0.5777		1.7293
Weiner		1.1554		0.7446

Though the mean values of the metrics are recorded in the tables, it is required to study the SSIM metric individual to the subbands as it reveals the degree of closeness between any 2 images. The MATLAB plots of the SSIM metrics of the recovered images after extraction of 32x32 and 64x64 watermarks are shown in the Figure 9 and Figure 10 respectively. The SSIM values are found to be closer to 1 and imply the similarity of the reconstructed images to the respective original images irrespective of the candidate subband.
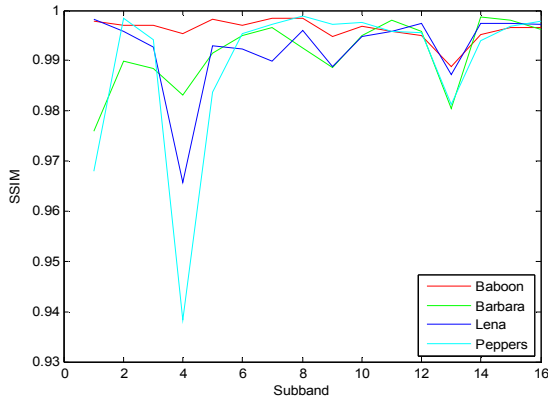

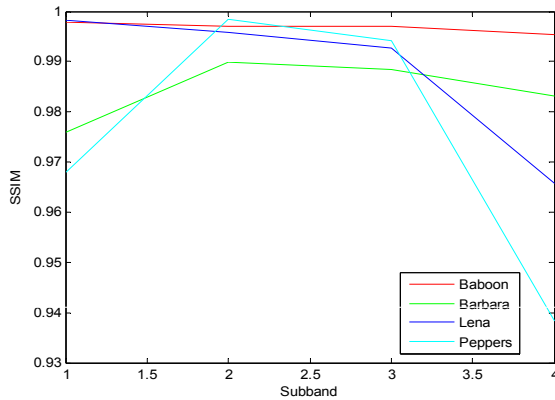**Fig 9: SSIM - Recovered Images after 32x32 Logo Extraction**

Fig 10: SSIM - Recovered Images after 64x64 Logo Extraction

7. DISCUSSION

The results detailed in the previous section indicate that the proposed system provides better imperceptibility and fidelity as evidenced from the PSNR and WPSNR values. The values of SSIM, MSSIM and UIQI metrics that are closer to 1, invariably for both 32x32 and 64x64 embedding apparently indicate that the system proposed can be used for watermarking highly sensitive images without compromising quality. However, the system is not resistant to cropping, shearing and compression attacks. Different watermarking schemes employ different approaches for watermark embedding and extraction, and varied metrics for performance evaluation. They also select different cover images and watermark patterns of different sizes for implementation of the algorithms. The algorithms also differ with respect to the kind of domain chosen for watermarking.

Many schemes have been published for LSB embedding, wavelet subband embedding, countourlet embedding etc. The proposed schemes for contourlet domain watermarking differ from each other on the number of levels of decomposition and the number of directional subbands in each level. However, they follow a common approach in the selection of the candidate subband, i.e. the highest energy subband. The general requirements of any watermarking system such as capacity of watermark, imperceptibility of the watermarked image, fidelity of the recovered image and the robustness of the watermark can be achieved to only a reasonable degree, as each of the requirements lead to the deprivation of the other. The focus of the reversible watermarking schemes is the quality of the recovered image which can be measured by various fidelity metrics.

Though robustness is an essential feature to be supported by the watermarking systems, it cannot be achieved against various attacks to which the images are subjected to, as it depends upon the candidate coefficients chosen for watermarking which differs from one method to another. The schemes focusing on reversibility generally use PSNR and MSE values as fidelity measures. It has been shown that WPSNR, SSIM, MSSIM and UIQI measures provide a better correlation with the perception of the Human Visual System (HVS). Hence, these measures should be used by further schemes to evaluate the quality of the reconstructed images.

8. CONCLUSION

In this paper, we have proposed a blind and reversible watermarking system for authentication and copyright protection. The proposed scheme provides a good degree of imperceptibility and reversibility as evident from the experimental results. The proposed system follows embedding and extraction algorithms which are unique for any candidate subband. The proposed system can be compromised by an attacker to capture the hidden watermark, only with the knowledge of the scalar constant *const* used in watermark embedding, number of levels of contourlet decomposition, number of directional subbands in each level, candidate subband, number of iterations and the initial conditions of the Arnold transform. Any attempts to extract the hidden watermark by brute force approach, assuming different values of these parameters will be highly time consuming. The blind extraction featured by the system is significant as it eliminates the need for exchange of the host image. Our future work is to improve the robustness of the scheme to geometric attacks, by identifying the candidate coefficients invariant to geometric transformations. Further the proposed approach can be extended to embed color watermark images within color host images.

9. REFERENCES

[1] Honsinger, C., Jones, P., Rabbani, P. and Stoffel, M. 1999. Lossless recovery of an original image containing embedded data,US Patent application, Docket No: 77102/E-D.

[2] Fridrich, J., Goljan, M. and Du, R.2001. Invertible Authentication, Proc. SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, January 23−26.

[3] Tian, J., 2002. Reversible watermarking by difference expansion, Proceedings of Workshop on Multimedia and Security.

[4] Li, H. F. and Wen, J. T. 2006. A Novel Blind Watermarking Algorithm in Contourlet Domain, IEEE International Conference on Pattern Recognition.

[5] Do, M., Vetterli, M., 2002. Contourlets: a directional multi resolution image representation, IEEE International Conference on Image Processing, Rochester, vol. 1, pp. 357–360.

[6] Dr.Peterson.2001.Triangular Number. http://mathforum.org/library/drmath/view/56036.html

[7] Gabriel Peterson.1997.Arnold's Cat Map,Math45-Linear algebra http://online.redwoods.cc.ca.us/instruct/darnold/maw/catmap.htm

[8] Duncan, D., Po, Y. and Minh N. Do, 2006. Directional Multiscale Modeling of Image Using the Contourlet Transform, IEEE Transactions On Image Processing, Vol. 15, No. 6.

[9] Sahraeian, S. M. E., Akhaee, M. A. , Hejazi, S. A. and Marvasti, F. 2008. Contourlet based image watermarking using optimum detector in the noisy environment, IEEE ICIP, pp 429-432.

[10] Cox, I., Kilian, J., Leighton, F.T. and Shamoon, T. 1997 Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, vol. 6, pp. 1673-1687.

[11] Song, H., Yu, S., Yang, X., Song, L. and Wang, C. 2008. Contourlet-based image adaptive watermarking, Elsevier Signal Processing: Image Communication 162–178.

[12] Elham Salahi, Shahram Moin, M. and Ahmad Salahi, 2008. A New Visually Imperceptible and Robust Image Watermarking Scheme in Contourlet Domain, IEEE IIH-MSP, pp 457-460.

[13] Shereen Ghannam and Fatma Abou-Chadi E. Z., 2009. Enhancing Robustness Of Digital Image Watermarks Using Contourlet Transform, IEEE ICIP 3645-3648.

[14] Athanasios Nikolaidis and Ioannis Pitas.2000. Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2000 Geneva.

[15] Wu, X. and Guan, Z. H, 2007. A novel digital watermark algorithm based on chaotic maps, Physics Letters A, 365, Jun. 2007, 403-406.

[16] Lei-Da Li, Bao-Long Guo,2009. Localized image watermarking in spatial domain resistant to geometric Attacks, International Journal of Electronics and Communications, pp 123-131.

[17] Zhou Wang, 2002. A Universal Image Quality Index, IEEE Signal Processing Letters, vol. 9, pp. 81–84.

[18] Rabbani, H., Vafadust M. and Gazor, S., 2007. Medical Volume Noise Reduction Employing a Laplace Distribution with Local Variance for Modeling Contourlet Coefficients, Proceedings of the 4th IEEE-EMBS International Summer School and Symposium on Medical Devices and Biosensors.

[19] Jayalakshmi, M., Merchant S. N. and Desai, U. B. 2006. Digital Watermarking in Contourlet Domain, Proceedings of the 18th International Conference on Pattern Recognition (ICPR2006), vol.3, pp.861-864.

[20] Shelby Pereira, Sviatoslav Voloshynovskiy, Maribel Madueño, Stéphane Marchand-Maillet and Thierry Pun, 2001. Second generation benchmarking and application oriented evaluation, Information Hiding Workshop, Pittsburgh, PA, USA.