ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

Watermark insertion and detection using contourlet and wavelet transforms

SHUBHRA BANERJI[1], Dr. AVIJIT KAR[2]

Senior Manager in their Software Testing Research & Development Unit,IBM India private limited, Bangalore, India[1]

Professor of Computer Science and Engg. Jadavpur University, Kolkata , India[2]

Abstract: Digital watermarking is now an established & cost effective method for data authentication and for protection of multimedia data. Many standard and commercially available software are available for this purpose. In this paper an attempt has been made to modify the method of Reddy and Chatterji [13, 14] by using contourlet transform for the watermark signal. The theoretical background of the method along with the simple development of the contourlet transform has been given. The algorithms for watermark insertion and detection are provided. The method was used for many different types of images and watermarks. A set of five such results are given along with the PSNR (peak signal to noise ratio) values of watermarked images and the detected watermarks.

Keywords: Contourlet transform HVS characteristics, Laplacian pyramid decomposition, directional filter bank, covariance of watermark coefficients.

1. INTRODUCTION

Watermark is a small and usually invisible signal which is inserted into a host image or signal so that it will be always there in the image or signal and can be detected whenever necessary. Sometimes the watermark is a logo and sometimes it can be biometric signal. This is used for the purpose of security. Watermarking got importance because the watermark signal is usually not removed during signal and image processing as well as during transmission, reception, storage and other operations.

We have seen the watermarking of some visual marks in currency notes and papers [16] which is currently extended in multimedia data [9] using digital technology. There are many applications of watermarking. Some of these are (i) Copyright protection – here owner's information or company logo is embedded as watermark using some key to protect the intellectual property and the watermark can be extracted to give the proof of the ownership whenever needed. (ii) Data authentication – here watermarking is used for verifying the content integrity and tamper detection. A fragile watermark is used during embedding and it is possible to detect the distortion of data and the tampered regions because there will be modifications in the extracted watermarks in those regions. (iii) Copy protection – as used in DVD copy protection the watermark embedded in the information is helpful in deciding whether to allow the materials to be copied or not [2,10]. (iv) Fingerprinting – here in addition to the owner's information, the customer's information is also embedded as watermark which is used to find the source of illegal copy. (v) Indexing – hare comments, markers or key information are embedded as watermark in the video database and these are used in search engine for unambiguous and quick data recovery. (vi)Medical application – here patient's name or other details are embedded as watermark in such a way that it does not interfere with medical examination by Doctors and these are used in unambiguous searching of medical

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

records. (vii) Broadcast monitoring – watermark is embedded in commercial advertisement for verifying in automatic monitoring system and for protecting valuable information from illegal transmission.

There several requirements of watermarking [13]. Some of these are (a) Imperceptibility – which means embedding of watermark should not degrade the quality of the host data appreciably. PSNR (Peak signal to noise ratio) between original and watermarked data is used as a measure for judging then degradation of the quality. (b) Robustness towards intentional and unintentional attacks. Sometimes maliciously people try to modify the contents of data and thereby the watermark. Some examples are signal processing operations like filtering and compression, warping and collision attacks. (c) Unambiguous detection – here the embedding and extraction process should be simple and provide transparent detection so that non-technical arbitrator is easily convinced. (d) Payload and capacity – here payload is defined as the amount of watermark information which can be inserted in the host data and capacity is the amount data which can be inserted and detected without error. (e) Security – Unauthorized parsons should not see, modify or remove the logo or other information used as watermark. Kerckhoff's principle [8] suggests that the watermarking embedding and detection methods should be known and the choice and type of key should decide the security. The watermark should be discreet /statistically invisible so that it cannot be removed by unauthorized persons. (f) Oblivious and non- oblivious watermarking – if original image is needed during watermark detection then the process is non-oblivious. On the other hand in oblivious watermarking the original image is not used during watermark extraction. Non-oblivious methods provide robustness, but in many applications the original image may not be available. (g) False positive and false negative detection probabilities – if watermark is present and not detected during extraction it is called false negative detection and on the other hand if there is watermark detection in the absence of any watermark then it is called false positive detection. The probabilities in both the cases should be as small as possible. There are several watermarking and detection methods like spread spectrum based methods, discrete cosine transform based methods, discrete wavelet transform (DWT) methods, quantization based methods etc. Depending on the application and depending on the requirements one has to decide the method. But now-a-days one prefers to use DWT based methods. The next section will describe one such technique which has been used in this work. The method is the modification of a standard method [14] by incorporating contourlet transform for the watermark image. Section 2 provides the details of the method and the theoretical backgrounds. Section 3 provides the experimental results and a brief conclusion is given in section 4.

2. WATERMARKING METHOD

The method presented in this section inserts a grey scale logo or some visual identity to the original image in the wavelet domain. The method is non-oblivious and hence during the watermark detection the original image is required [3,17].
The method uses the human visual system characteristics (HVS) for watermark embedding as well as for watermark detection. The method is a modification of the Reddy and Chatterji's algorithm [13, 14, 15]. In their algorithm both the input image and logo are transformed into the wavelet domain. In this modified method the input image is transformed into wavelet domain using three level discrete wavelet transform (DWT), but one level discrete contourlet transform is used for the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

logo image. The main reason for selection of discrete contourlet transform [5] is its directionality and anisotropy properties. It is well known that the logo selected by the user is usually a simple small image and has directional information with smooth contours. Contourlet transforms are better for such image because it represents the information in less number of coefficients as compared to wavelet transform. Do & Vetterli [6] in their development of contourlet transform used the Laplacian pyramid (LP) of Bert and Adelson [4] to get the point discontinuities. These discontinuities are then used in a directional filter bank (DFB) to obtain linear structures. This can be extended at various scales. Contourlet transform has elongated supports not only at various scales but also at various directions and at various aspect ratios. In brief one can say that contourlet transform has directionality property because its basis elements have orientation in more directions. It has anisotropy property because its elements have number of elongated shapes having different aspect ratios. The one level Laplacian pyramid decomposition and directional filter banks decomposition of contourlet transform [6] are given in Fig. 1 and Fig. 2.

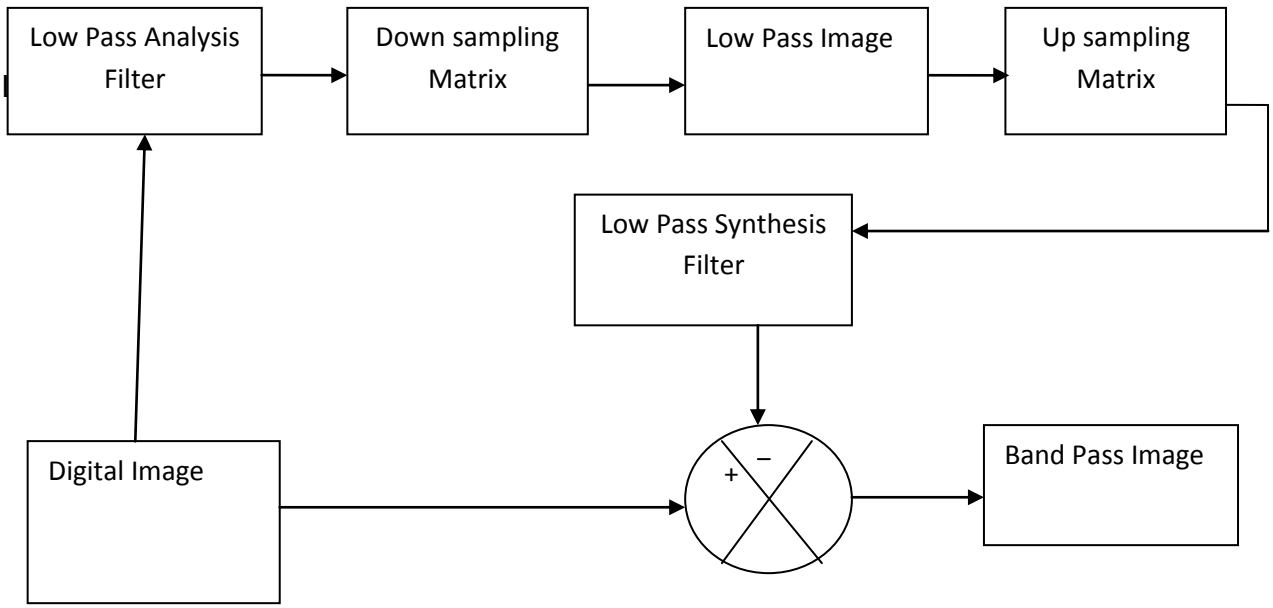

Fig. 1. One level Laplacian Pyramid Decomposition

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

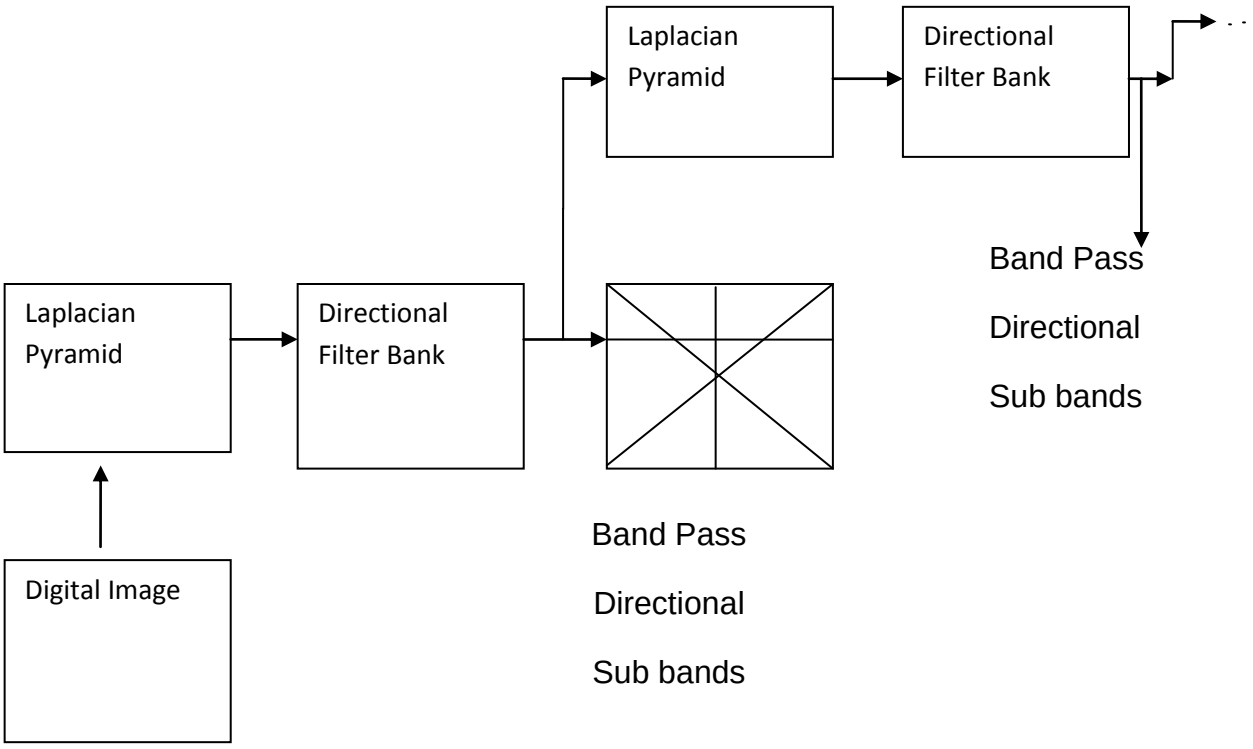

Fig.2. Directional Filter Bank Decomposition

In Fig.1 Laplacian pyramid decomposition is obtained using one dimensional low pass analysis filter, down something matrix, upsampling matrix and low pass synthesis filter. This provides a band pass image. This can be extended to next and higher levels. The directional filter bank decomposition (DFB) as shown in Fig.2 is used to obtain high frequency content in the form of edges along directions and smooth contours. The method for implementation of DFB was given by Po and Do [11]. A simplified method was given by Bamberger and Smith [1] which was used by Srinivas Rao et al [12] for computer based image retrieval CBIR. The combination of Laplacian pyramid and DFB is called the contourlet transform. Here band pass image is fed to DFB block to obtain directional information. This can be repeated at different level of coarse image thus obtaining directional sub-bands at multiply scales.

The block diagrams of the watermark insertion and detection processes are shown in Fig. 3 and Fig. 4 respectively. Here the input image is transformed into wavelet domain and the watermark image (logo) is transformed into contourlet domain. Three level DWT is used for the input image whereas one level discrete contourlet transform is used for the logo image. One level decomposition is better because it was found that at higher levels the sub bands are more sensitive to noiseand distortions due to the presence of more coefficients in the extracted logo. The transformed watermarks are inserted in the sub bands using weights according to the procedure mentioned in the next paragraph. 3 – level IDWT (inverse discrete wavelet transform) is used on this image to obtain the watermarked image in spatial domain. For the detection of watermark 3 – level DWT operation is done in both the watermark image and the input image. In the wavelet domain the watermark image is obtained by the inverse process of watermark insertion. Then inverse discrete contourlet transform is used to obtain the watermark which is compared with the original watermark to determine whether it is actually present or not.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

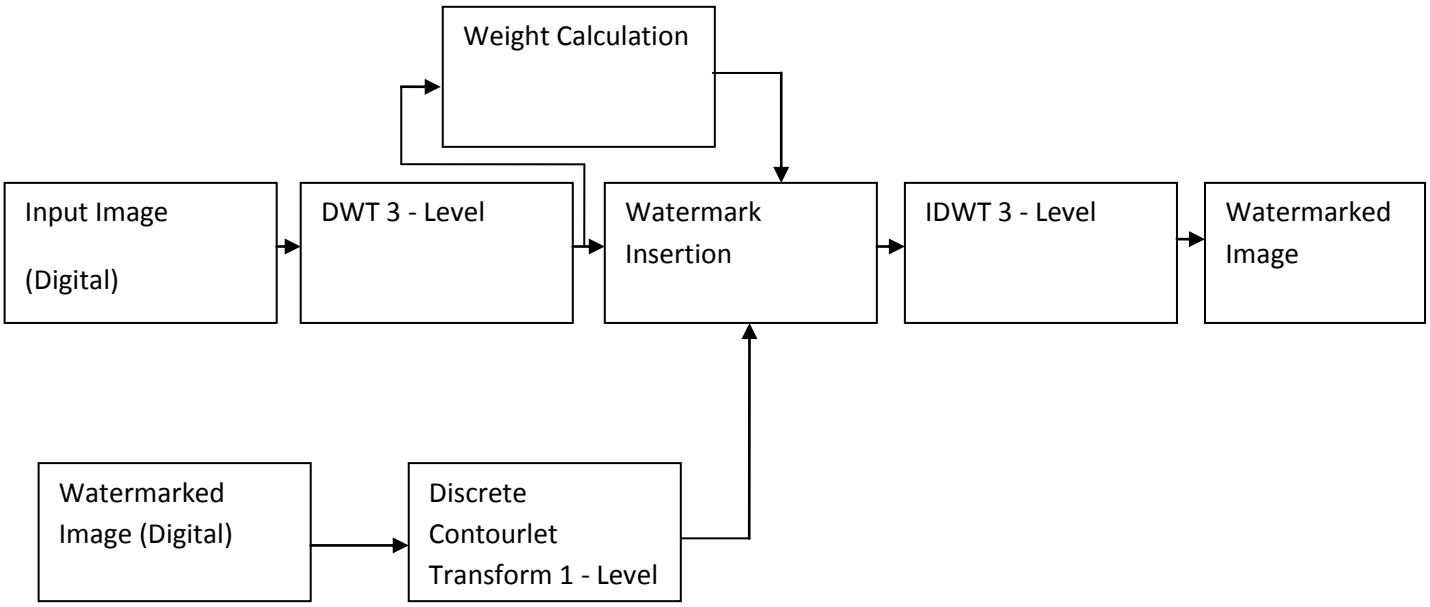

Fig. 3. Block Diagram of Watermark insertion Method

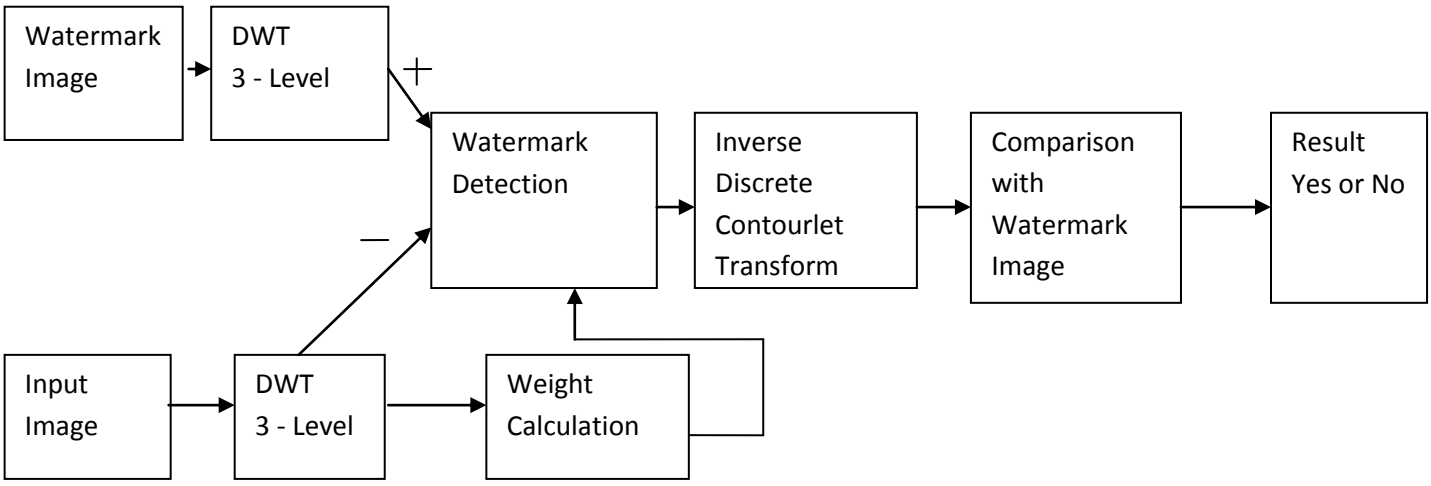

Fig. 4 Block Diagram of the watermark detection method

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

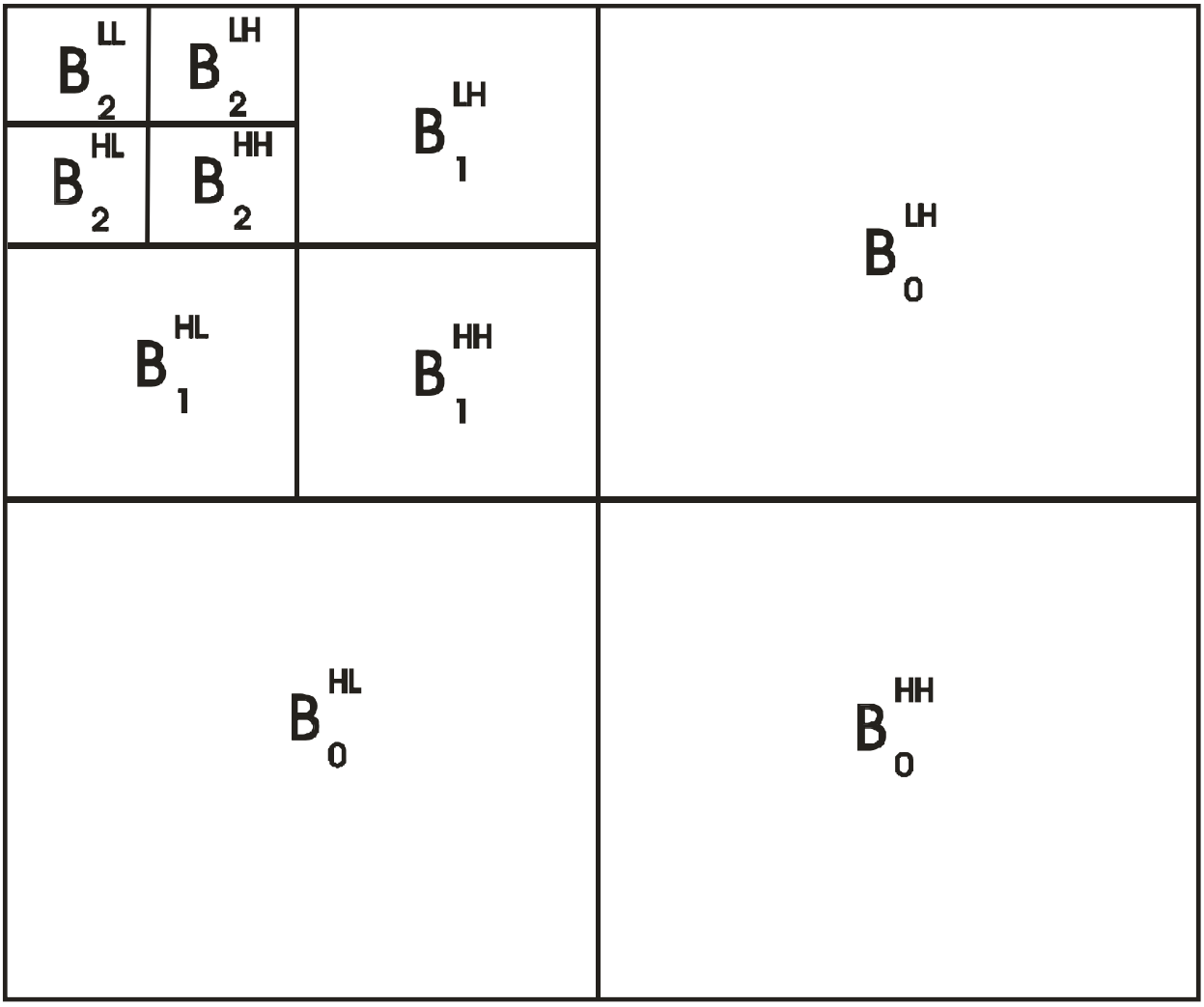

Fig. 5 Decomposition of the input image for 3 – level DWT

Fig. 5 shows the 3-level DWT decomposition of the image. Here $B_n^k(i,j)$ represent each sub band where $l \in \{0,1,2\}$ and $k \in [LL, LH, HL, HH]$ considering noise sensitivity of human eye to frequency orientation, luminance and texture, the weights are calculated using the following equations [13]

$$w_n^k(i,j) = \frac{1}{2} F(n,k) L(n,i,j) T(n,i,j)^{0.2} \quad \ldots\ldots\ldots\ldots (1)$$

The noise sensitivity of eye to level and orientation is given by

$$F(n,k) = \begin{cases} \sqrt{2} & \text{if } k = HH \\ 1 & \text{otherwise} \end{cases} X \begin{cases} 1.00 & \text{if } n = 0 \\ 0.32 & \text{if } n = 1 \\ 0.16 & \text{if } n = 2 \end{cases} \quad \ldots\ldots\ldots\ldots (2)$$

The effect of luminance is accounted for using the following equations

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

$$S'(n,i,j) = \frac{1}{64} B_n^{LL}(i,j) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$S'(n,i,j) = \begin{cases} 1-S(n,i,j) \text{ if } S(n,i,j) < 0.5 \\ S(n,i,j) \text{ otherwise} \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$L(n,i,j) = 1 + S'(n,i,j) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

The sensitivity to noise in the texture areas is calculated using the following equation

$$T(n,i,j) = \sum_{m=0}^{2-n} \frac{1}{8^m} \sum_{k=0}^{LH,HL,HH} \sum_{x=0}^{1} \sum_{y=0}^{1} \left[B_{m+1}^{k}\left(x + \frac{i}{2^m}, y + \frac{i}{2^m} \right) \right]^2 x \text{ Var} \left\{ B_n^{LL}(x+i, y+j) \right\}_{\substack{x=0,1 \\ y=0,1}} \quad \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

The watermark insertion process involves addition of the watermark coefficients with image coefficients in 1-level sub band according to the following equation.

$$\hat{B}_n^k(i,j) = B_n^k(i,j) + \alpha \omega_n^k(i,j) + C(i,j) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (7)$$

Where C (i,j) is the discrete contourlet transform coefficients of the logo image, $\hat{B}_n^k(i,j)$ is the watermarked coefficients in DWT domain and α is a constant representing watermark strength. During watermark detection inverse operation is done. First the transformed coefficients are determined using the following equation (vide Fig.4)

$$\hat{C}(i,j) = \frac{\hat{B}_n^k(i,j) - B_n^k(i,j)}{\alpha\, \omega_n^k(i,j)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (8)$$

The extracted logo $\hat{G}(x,y)$ is the inverse contourlet transformation of $\hat{C}(i,j)$. This is compared with original logo. One can use covariance $\rho(G,\hat{G})$ between the original and extracted watermark image using the following equation

$$\rho(G,\hat{G}) = \frac{\sum_{I=1}^{N^2} G(i)\,\hat{G}(i)}{\sqrt{\sum_{i=1}^{N^2} G^2(i)}\,\sqrt{\sum_{i=1}^{N^2} \hat{G}^2(i)}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9)$$

Here N2 is the total number of pixels in the logo. If this covariance $\rho(G,\hat{G})$ is above a threshold we consider watermark is present otherwise we conclude that watermark does not exist.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

3. EXPERIMENTAL RESULTS

The watermark insertion and detection methods as given in previous section and as depicted in Fig. 3 and Fig. 4 were experimented using several different types of images and watermarks. In this section the results of five such experiments will be illustrated. The images are 8 bit grey scale of size 512X512 whereas the watermarks are 64X64 size images of 8 bit grey scale. Fig. 6 shows the experimentation of standard Lena image Fig.6 (a) using a twitter image Fig. 6 (b) as the watermark. Three level wavelet decomposition was used for Lena image using Daubcchies 9/7 filter coefficients. One level contourlet decomposition was used for the watermarked image. The watermarked Lena image is shown in Fig.6 (c). From this watermarked image the watermark was extracted using the algorithm shown in Fig. 4. The detected twitter watermark is shown in Fig. 6 (d).Fig.7 (a) shows a 512X512X8 bit alphabet image, This was watermarked using 64X64X8 bit circle image shown in Fig. 7 (b). The watermarked image is shown in Fig. 7 (c) and the detected watermarked is shown in Fig.7 (d). Fig.8 (a), 8 (b), 8 (c) and 8 (d) show the 512X512X8 bit Taj Mahal image, 64X64X8 Olympic symbol image as watermark, watermarked image and the extracted watermark respectively. Similarly Fig.9 (a), 9 (b), 9 (c), and 9 (d) show the 512X512X8 bit flower image, 64X64X8 ring watermark image, watermarked flower image and the extracted (detected) watermark image. Finally Fig.10 (a), Fig.10 (b), Fig. 10 (c) and Fig.10(d) show the 512X512X8 bit nature scene image, 64X64X8 bit adobe watermark image, watermarked scene image and the detected image respectively.

(a)Lena Image (b)Twitter Watermark (c)Watermarked LenaImage (d)Detected Twitter Watermark

Fig 6

(a)Alphabet Image (b)Circle Watermark (c)Watermarked Alphabet Image (d)Detected Circle Watermark

Fig 7

(a)Tajmahal Image (b)Olympic Symbol Watermark (c)Watermarked Tajmahal Image (d)Detected Olympic Symbol Watermark

Fig 8

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

(a)Flower Image (b)Ring Watermark (c)Watermarked Flower Image (d)Detected Ring Watermark

Fig 9

(a)Nature Scene Image (b)Adobe Watermark (c)Watermarked Flower Image (d)Detected Adobe Watermark

Fig 10

It may be noted that the watermarked images Fig.6 (c), Fig.7 (c), Fig.8 (c), Fig.9 (c) and Fig.10 (c) will differ from the original image Fig.6 (a), Fig.7 (a), Fig.8 (a), Fig.9 (a) and Fig.10 (a) respectively.

Similarly the extracted watermarks Fig.6 (d), Fig.7 (d), Fig.8 (d), Fig.9(d) and Fig.10 (d) will differ from the original watermarks Fig.6 (b),Fig.7 (b), Fig.8 (b),Fig.9 (b) and Fig.10 (b) respectively. The difference or degradation is estimated using the standard measure called PSNR or peak signal to noise ratio. For an 8 bit grey scale image (which is the case in this experimentation) PSNR is defined as

$$PSNR = 20\log_{10}(255) - 10\log_{10}\left[\frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(O(i,j)-D(i,j))\right] \quad \ldots\ldots\ldots\ldots\ldots\ldots (10)$$

Where O (I,j) and D (I,j) are the original and degraded images each of size NxN. PSNR was estimated for watermarked images and the detected watermarks of all the above five cases. Table – 1 gives the PSNR values of the watermarked images and the extracted watermarks of the images of experimentation.

Table – 1 PSNR values of Watermarked Images and Detected Watermarks

Image	Watermark	PSNR value of the Watermarked image	PSNR value of the Detected Watermark
Lena	Twitter	42.14 dB	35.17 dB
Alphabet	Circle	45.67 dB	34.32 dB
Tajmahal	Olympic symbol	43.26 dB	36.82 dB
Flower	Ring	46.79 dB	37.46 dB
Scene	Adobe	44.90 dB	33.52 dB

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

The watermarked images were tested for different geometric attacks like resizing, cropping etc. and non-geometric attacks like filtering, histogram equalization and compression etc. It was found that the detection process can extract the watermark within reasonable accuracy.

4. CONCLUSION

Digital watermarking of images is well established technique for images. Many standard and commercially available software are available and these are in use for many applications. This paper attempted modification of a standard method by using contourlet transform for the watermark image. The method uses human visual system characteristics [13]. By looking at experimental results, the detected watermark images and at PSNR values given in Table – 1 one can be sure of the acceptability of the method. As an extension of the work one can try other transforms and can give a comparison of the method using these transforms in terms of quality of the detected watermark and the tolerance under various attacks.

REFERENCES

1. R.H.Bamberger and M.J.T.Smith. A filter bank for directional decomposition of images: theory and design, IEEE Trans. On Signal Prosessing, Vol. 40, No-4, p 882-893, April 1992.
2. J.A.Bloom, I.J.Cox, T.Kalker, J.M.G.Linnartz, M.L.Miller and C.B.S Traw, Copy protection for DVD Video, Proc. of the IEEE, 87,p1267-1276, July 1999.
3. G.W.Braudaway, Protecting publicly available images with an invisible image watermark, Int. Conf. on Image Processing, p.524-527, Oct. 1997.
4. P.J.Burt and E.H.Adelson, Laplacian pyramid as a compact image code, IEEE Trans. on communication, Vol. 31, No.4, P 532-540, April 1983.
5. M.N.Do, Directional multiresolution image representation, Ph.D dissertation, School of Computer and Communication Science, Swiss Federal Institute of Technology, Laussanne, Switzerland, 2001.
6. M.N.Do and M.Verrerli, The Contourlet Transform: An efficient directional multiresolution image representation, IEEE Trans. On Image Processing, Vol. 14, No.12, p 1-16 Dec. 2005.
7. A.K.Jain and U.Uludag, Hiding biometric data, IEEE Trans. on Pattern Analysis and Medicine Intelligence, Vol. 25, No.11, p. 1494-1498, Nov.2003.
8. A.Kerckhoffs, La Cryptographic militaire, Journal des Sciences Militaires, Vol.9, No.1, P 5-38, Jan.1883.
9. D.Kundur, Multiresiolution digital watermarking algorithms and applications for multimedia signal, Ph.D Thesis, University of Toronto, Canada, 1999.
10. M.Maes, T.Kaller, J.P.Linnartz, J.Talstra, G.Depovere and J.Haitsma, Digital watermarking for dvd video copy protection, IEEE Signal Processing Magazine, p 1-10, Sept. 2000.
11. D.Y.Po and M.N.Do, Directional multiscale modeling of images using the contourlet transform, IEEE Trans. On Image Processing, Vol. 15, No. 6, p 1610-1620, June 2006.
12. C.S.Rao, S.S.Kumar and B.N.Chatterji, Content based image retrieval using contourlet transform, ICGST – GVIP Journal, Vol.7, No.3, p 9-14, Nov. 2007.
13. A.A.Reddy, Wavelet based watermarking techniques for digital images, Ph.D thesis, Indian Institute of Technology, Kharagpur.India, 2005.
14. A.A.Reddy and B.N.Chatterji , A wavelet based robust logo watermarking scheme, Int. Conf. on Advances in Pattern Recognition, p.359-362, Kolkata, India, Dec.2003.
15. A.A.Reddy and B.N.Chatterji, A new wavelet based logo watermarking scheme, Pattern Recognition Letters, Vol. 26, No. 7, p.1019-1027, 2005.
16. B.Rudin, Making paper- A look into the history of an ancient craft, Vallingly, Sweden, 1998.
17. B.L.W. Zeng and S.Lee, Extraction of multiresolution watermark images for resolving rightful ownership, Proc. of SPIE Security and watermarking of Multimedia Contents, Vol. 3657, p.404-414, Jan, 1999.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

BIOGRAPHIES

Shubhra Banerji is with IBM India Pvt. Ltd. as Senior Manager in their Software Testing Research & Development Unit.
She has a Masters Degree in Physics (Integrated M.Sc) from IIT Kharagpur. She is working for PhD at Jadavpur University In Software Testing.
She is the recipient of R.G. Chatterjee Memorial Gold Medal at IIT Kharagpur on being adjudged the best student in Grade Point Average, Project Work and Laboratory Practices.
She has 17 years of extensive software experience in Development and Testing in various Domains.
Earlier she was with Infosys Technologies Limited Bangalore where she was responsible for managing a group of 50 Test Engineers and Analysts to provide defect-free tested software to client and was involved in Estimation, Status Reporting, Metrics Analysis and Quality Management in her project.
Shubhra has presented a paper in "Quality Management in Software Testing "at the International Software Testing Conference organized by QAI in 2007.
Shubhra has presented a paper on "Digital Watermarking for Information Security in Applications" at Step-Auto Conference 2008 organized by ISQT.
Shubhra's paper "Project Client Relationship Management" has been selected for publication for PML, 2008 organized by QAI.
Shubhra has presented a Tutorial on "User Acceptance Testing: The Right Way" in StePIN 2009.
Shubhra has also published papers in various journals.
Shubhra can be contacted at: shubhra.banerji@gmail.com