using fully DFB decomposition on each band could compensate for the drawbacks of the wavelet filters. Figure 2 shows the flowchart of first level decomposition of WBCT on an image. The HF subband images from the WT are processed by the DFB so that the directional information can be captured. The scheme can be iterated the LF subband image over. The WBCT decomposes the image into directional subbands at multiple scales.

By analyzing, we find that WBCT can capture image structure features more efficiently than Discrete Wavelet Transform (DWT) and be more suitable to identify the subbands in the host image where a watermark can be embedded effectively. Considering a watermarking scheme that embeds watermark into HF subbands, which watermark will be removed easily when the watermarked image is attacked by image processing methods destroying the HF information of the image; while watermark is embedded in LF subbands which may make the scheme easily perceptible[10]. In order to ensure the visual quality and robustness of the image which watermark is embedded into, the watermark should be embedded into the low-middle frequency subbands in our scheme.

3.4.3 Embedding Algorithm

1 Perform L-level order decomposition using WBCT on image
2 Perform SVD on all the subbands of the randomized host image and the gray scale watermark
3 Modify the Singular values of all subbands with the help of singular values of the watermark
4 Perform inverse SVD to construct all modified subbands
5 Perform inverse L-level order decomposition of WBCT
6 Perform the inverse randomization to obtain the watermarked image

3.4.4 Watermark Extraction

The objective of watermark extraction is to obtain the estimate of the original watermark. The Watermark image is extracted from the watermarked image.

1 Perform L-level order decomposition using WBCT on image
2 Perform SVD on all the subbands of the randomized host image and the gray scale watermark
3 Extract the singular values of the watermark from each subband
4 Perform inverse SVD to construct the extracted watermarks from each subband

3.5 Attack Analysis

The transmission of the images over insecure communication channels introduces degradation in the images. Such degradation also affects the hidden information (watermarks) in the images. Therefore, the robustness of the proposed technique against degradation incurred by various intentional and unintentional attacks is studied. Generally, a good watermarking technique should be sufficiently robust against all these attacks[4]. To investigate the robustness, the watermarked image is verified and then attacked by; Median filtering the median filter is a nonlinear digital filtering technique, often used to remove noise. Such noise reduction is a typical pre-processing step to improve the results of later processing. Gaussian noise addition is properly defined as the noise with a Gaussian amplitude distribution. This says nothing of the correlation of the noise in time or of the spectral density of the noise. Salt and pepper noise addition is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels

4 Experimental Results

The performance of the proposed biometrics inspired watermarking framework is demonstrated using a MATLAB platform. A number of experiments are performed on different gray-scale images of size 256 × 256, namely Building, Lena and Mandrill. Also, three different gray-scale images of size 64×64, namely Logo1, Logo2 and Logo3 respectively, are used as the watermark images. Watermarks Logo1, Logo2 and Logo3 are embedded into Building, Lena and Mandrill images, respectively. The keys are obtained with the help of biometrics of the owner/user. Since biometrics are the unique and permanent characteristics of the individuals.

Therefore, biometrics inspired keys are unique and can only be generated by the owner/user. For the image watermark embedding, the 2-level of WBCT decomposition is used. Therefore, the watermark is embedded more than once in the host image. The watermarked image quality is measured using the peak signal to noise ratio (PSNR) which indicates the similarity between the host and the watermarked images[15]. To evaluate the similarity between the

original and extracted watermarks; the correlation coefficient (ρ) is used as the similarity measure between the original and extracted watermarks show in the Equation 4. Mathematically, ρ is defined as

$$\rho = \frac{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1}(w(i)-m_w)(\overline{w}(i)-m_{\overline{w}})}{\sqrt{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1}(w(i)-m_w)^2}\sqrt{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1}(\overline{w}(i)-m_{\overline{w}})^2}} \quad (4)$$

where w, $\overline{w}$, m_w and $m_{\overline{w}}$ are the original, extracted, mean of original, and mean of extracted watermarks respectively. ρ is a number that lies in the range [−1, 1].

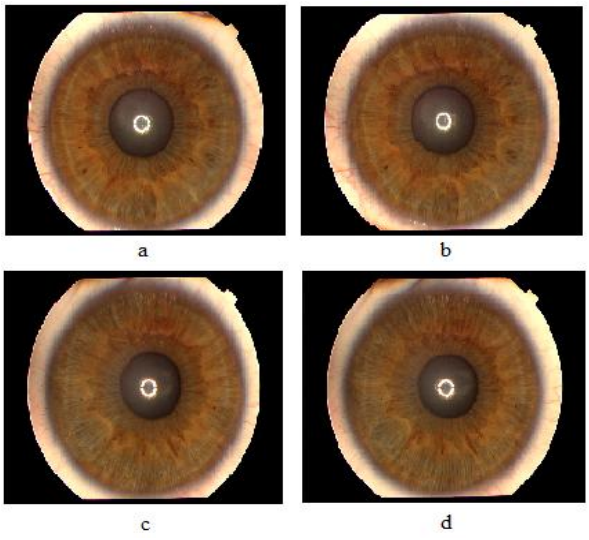

Figure 3 Iris images (a, b) Left Eye; (c, d) Right Eye

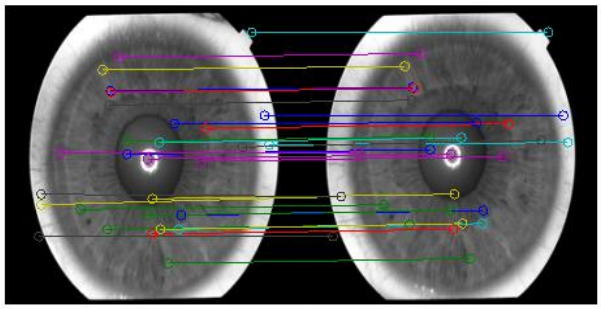

Figure 4 Interest Points Matching

The input Biometric Iris images of a person captured over a short period of a few seconds. Figure 3 depicts the iris images. The Figure 4 depicts Interest points matching. The input host image of size 256 × 256 is taken[9].

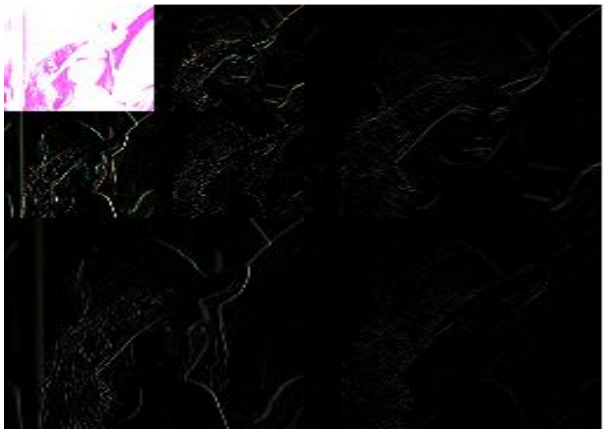

Figure 5 Applying Two Levels of WBCT Decomposition

Figure 6 (a, b, c) Original Host Images

Figure 6 depicts the original host images used for watermarking. Figure 5 depicts the two levels of WBCT Decomposition on the input host image. The Embedding of the watermark image with the host image to obtain the watermarked image is depicted in Figure 7. The most common manipulation in digital image processing is filtering. The attacked watermark image and extracted watermark, after applying 3 × 3 median filtering respectively, are shown in Figure 8 (a) and Figure 9 (a). Robustness against additive noise is estimated by degrading the watermark image by randomly adding Gaussian and salt and pepper noise. The attacked watermark images and extracted watermarks from the attacked images are shown in Figure 8 (b), Figure 9 (b) and Figure 8 (c), Figure 9 (c).

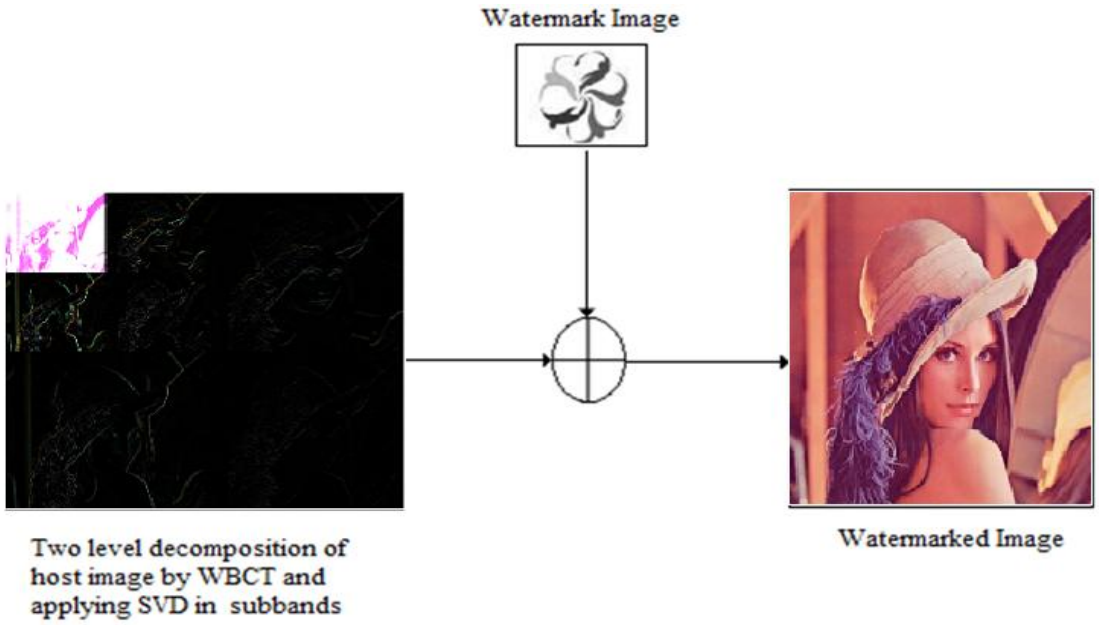

Figure 7 Watermark Embedding

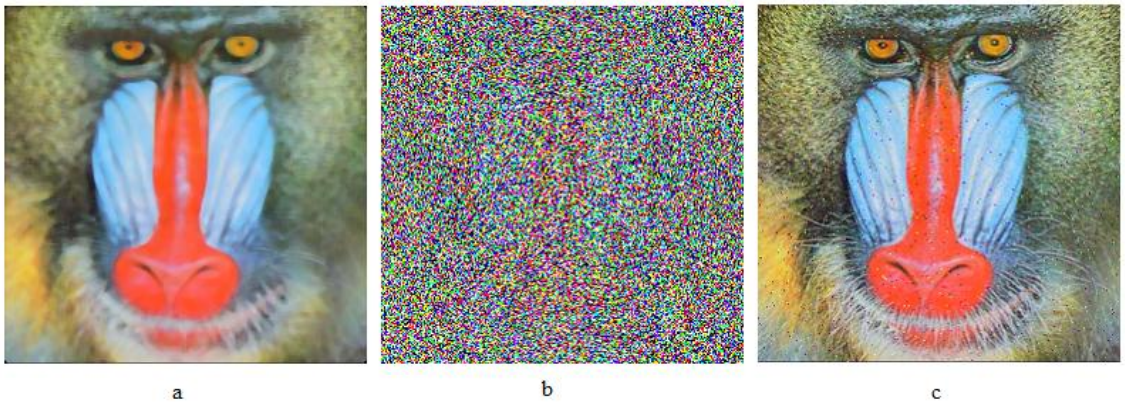

Figure 8 Watermarked Images after Attack (a) Median Filtering (b) Gaussian Noise Addition (c) Salt and Pepper Noise Addition

Figure 9 Extracted Watermark Images after (a) Median Filtering (b) Gaussian Noise Addition (c) Salt and Pepper Noise Addition

The Speeded-Up Robust Features (SURF) technique has been developed for both the detection and description of local features. The SIFT and SURF Techniques are applied on a dataset of 256 iris images. Table 1 represents the comparison rates of Sensitivity, Specificity and Execution Time.

Table 1 Comparison between SURF and SIFT

S.NO	Method	Sensitivity (%)	Specificity (%)	Accuracy (%)	Execution Time(in sec)
1	SIFT	71.1	93	72.7	1
2	SURF	98	72.7	89.4	0.8

The figures 10 describe the Execution Time Comparison of SURF and SIFT Techniques. The graph depicts that SURF provides less execution time than SIFT. In this paper, the SURF and SIFT techniques are evaluated in terms of Sensitivity (Se), Specificity (Sp) and Accuracy (Acc) as shown in the Equation 5, 6, 7. The comparison graph is shown in the Figure 11. Here TP-True Positive, FN-False Negative, TN-True Negative, FP- False Positive.

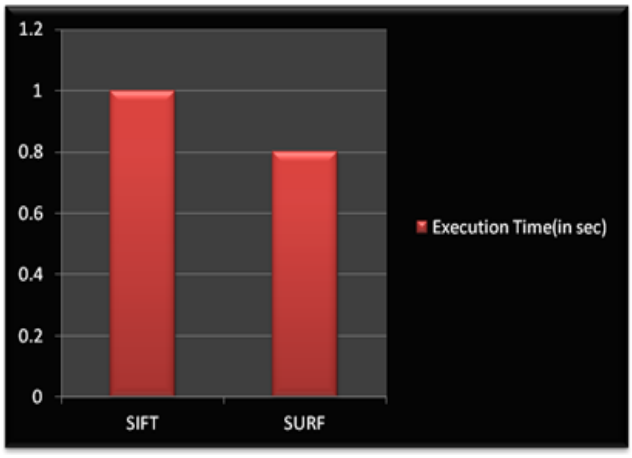

Figure 10 Execution Time Comparison of SURF and SIFT

The performance results [14] show the sensitivity (Se) of 98%. The correlation coefficients for all extracted watermarks are compared with other existing methods are depicted in Table 2 and Figure 12.

$$Se = TP/(TP+FN) \quad (5)$$

$$Sp = TP/(TN+FP) \quad (6)$$

$$Acc = TP+TN/(TP+FN+TN+FP) \quad (7)$$

Table 2 Comparison of Correlation Coefficients of Extracted Watermarks after Attack Analysis

Attacks	Multi-Band Wavelet	Contourlet	WBCT	WBCT+SVD
Median Filtering (3 × 3)	0.3557	0.4302	0.5545	0.8583
Salt and Pepper noise (0.01)	0.9193	0.9745	0.9807	0.9954
Gaussian Noise (10)	0.9087	0.9491	0.9657	0.9969

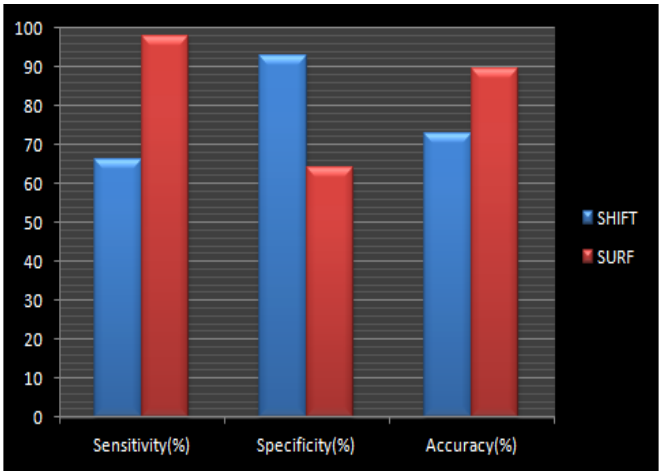

Figure 11 Comparison of Sensitivity, Specificity and Accuracy of SURF and SIFT

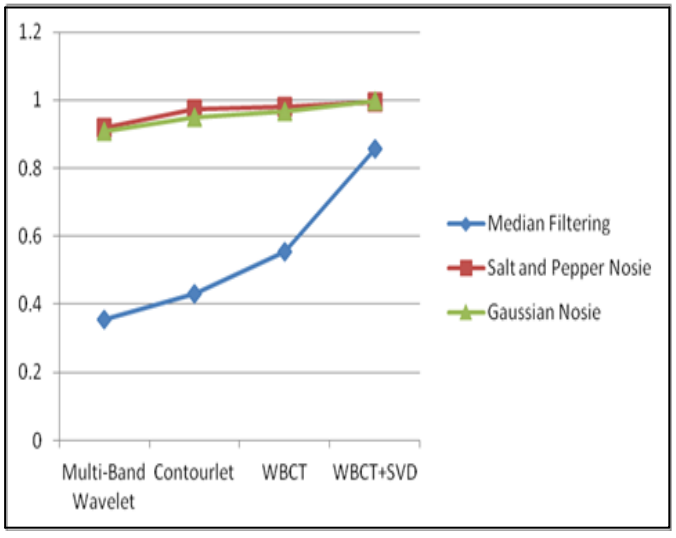

Figure 12 Correlation Coefficient Comparisons of Extracted Watermarks

5 Conclusion

The Biometrics trigged watermarking of images based on WBCT is proposed in which the key concept is introduced with biometric security. The original image has been improved by optical inspection. An Efficient method SURF is used for the feature extraction and interest points matching. The SURF performance is shown in the comparative

analysis which is efficient in both retrieval time and feature extraction. Two level decomposition of the image is performed with the WBCT which is embedded with the biometric keys. Thus, the WBCT can give the anisotropy optimal representation of the edges and contours. The watermarked image is obtained by embedding the host image and the watermark image. The proposed technique meets the requirements of Digital Watermarking. As our experimental results have shown, the proposed algorithm achieves invisibility and robustness.

References:

[1] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, Vol. 3, No. 9, 2001, pp. 740-746.

[2] H. Bay, T. Tuytelaars, L. Van Gool, "SURF: Speeded Up Robust Features", in:Proc. Computer Vision and Image Understanding,Vol.110, No.3, 2008, pp. 346-359.

[3] Gaurav Bhatnagar, Q.M Jonathan Wu, "Biometrics Inspired Watermarking Based on a Fractional Dual Tree Complex Wavelet Transform", Future Generation Computer Systems, Vol. 29, 2013, pp. 182-195.

[4] A.K. Jain, "A. Ross: A Tool for Information Security", IEEE transactions on Information Forensic and security, Vol.1, No. 2, 2006, pp. 125-143.

[5] A.k. Jain, R. Bolle, S. Pankanti, "Biometrics: Personal Identification in a Networked Society", Kluwer Academic Publishers, 1999.

[6] Jing Liu, Gang Liu, "A New Digital Watermarking Algorithm Based on WBCT", International Workshop on Information and Electronics Engineering (IWIEE), 2012, pp. 1559 – 1564.

[7] G.C. Langelaar, I. Setyawan, R.I. Lagendijik, "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, Vol. 17, No. 5, 2000, pp. 20-46.

[8] Z.M. Lu, D.J. Xu and S.H Sun, "Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization", IEEE Transactions on Image Processing, Vol. 14, No. 5, 2005, pp. 3271-84.

[9] Michal Dobes, Libor Machala, Iris database. http://www.inf.upol.cz/iris/

[10] Roy K, Bhattacharya P," Iris Recognition: A Machine Learning Approach", VDM Verlag Saarbrücken, Germany, 2008.

[11] Yavuz E, Telatar Z,"Improved SVD–DWT Based Digital Image Watermarking Against Watermark Ambiguity" in: Proc. ACM Symposium on Applied Computing, pp. 1051 – 1055, 2007.

[12] Chang-Doo Lee, Bong-Jun Choi, Kyoo-Seok Park, "Design and Evaluation of a block Encryption algorithm using dynamic-key mechanism", Future Gener. Comput. Syst., Vol. 20, No. 2, 2004, 327-338.

[13] Fabian Monrose, Aviel D. Rubin, "Keystroke dynamics as a biometric for authentication", Future Gener. Comput. Syst., Vol. 16, No.4, 2000, pp.351-359.

[14] A. Tefas, A. Nikolaidis, V. Solachidis, S. Tsekeridou, I. Pitas, "Performance analysis of correalation-based watermarking schemes employ markov chatic sequences", IEEE trans. Signal Process, Vol.51,2003, pp. 1979-1994.

[15] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE trans. Image Process", Vol.13, 2004, pp. 600-612.