



## BIOMETRIC WATERMARKING OF IRIS BASED ON SVD AND WAVELET

PRIYANKA JAWALE<sup>1</sup>, Dr. P.M.MAHAJAN<sup>2</sup>

<sup>1</sup>M. E. Student, <sup>2</sup>Professor

J. T. Mahajan College of Engg. Faizpur



### ABSTRACT

The main objective of this work is to describe an accurate, reliable and robust security system to hide an iris image and a key into a cover image and this objective will be achieved with three phases as described below. First iris biometric template is generated and values of templates are extracted through Gabor filter. Second the host image is thus firstly applied with the Haar wavelet transform followed up by the singular value decomposition of the sub band coefficients. At last for the extraction of the watermark from the stego image, the corrupted version of the watermarked image is received. Similar to the embedding process, the haar wavelet transform of the image is taken to obtain the corrupted image's sub bands. The process is explained in remaining sections of this paper. Implemented algorithm has been tested with popular attacks for analysis of false recognition and rejection of subject.

Keywords- Digital watermarking, image watermarking, watermark, discrete wavelet transform (DWT), singular value decomposition (SVD), biometrics, Hamming Distance, Normalized Cross Correlation (NC).

©KY Publications

### I. INTRODUCTION

Biometric watermark is a technique that creates a link between a human subject and the digital media by embedding biometric information into the digital object. Watermarking biometric data is growing importance and is under research for authentication systems. According to Low et al. [1], biometric watermarking was introduced as the synergistic integration of biometrics and digital watermarking technology. In the battle of copyright piracy, several technological approaches and solutions have been suggested and implemented in [2]. The watermark is nowadays used in conjunction with several biometrics including fingerprint [3], signature [4], face [5], hand [6], voice[7], retina[8]. Choice of biometric technology should also include consideration of the following parameters, taking

into consideration of the operational requirements. The parameters are Accuracy, Environment e.g. fully deployed battlefield, Ergonomics/ User-friendly, Stability and uniqueness of feature to be measured, Secure, Safety, Speeds of enrolment and recognition, Non-intrusiveness, Convenience, Cost, Size of stored template, Operational limitations e.g. finger and facial recognition through Nuclear Biological, Chemical/Chemical Biological Radiation clothing, Requirement ability to perform both identification and verification, Credible scientific background research, Human Acceptance and Robust. After consideration of all of the aforementioned biometric technologies, Iris is taken for our research work.

However, as the need for security increases, research for more permanent form of

biometric, which is difficult to replicate, is considered. One such biometric is human iris. Iris recognition is based on visible features, i.e. rings, furrows, freckles, and corona and is considered very challenging, as they possess a high degree of randomness. The Iris is completely formed by 8th month of adults, and remains stable through life. Statistically more accurate than even DNA matching since the probability of 2 irises being identical is 1 in 10 to the power of 78 [9]. Iris is unique and best biometrics that is mainly used for the establishment of instant personal identity [10]. Compared with other biometric technologies, such as face, speech and finger recognition, iris recognition can easily be considered as the most reliable form of biometric technology [11]. However, they are susceptible to accidental and intentional attacks, when transmitted over network. Thus, a protective scheme is needed which will preserve fidelity and prevent alterations. This is more important with respect to biometric identifiers because of their uniqueness. A good solution to this situation is watermarking [12]. Several techniques exist for the protection of biometric data but this paper discusses a technique that integrates iris and digital watermarking for authentication reasons. Combining digital watermark and biometric for authentication is an emerging area. The proposed algorithm was trained and evaluated on the dataset of 10 iris images using parameters like MSE, PSNR, False rate, Hamming Distance, NC.

The rest of the paper is organized as follows. Section 2 consists of proposed methodology. Section 3 consists of performance parameters. Section 4 consists of results and discussions. The conclusion is drawn in Section 5.

## II. PROPOSED SCHEME

A. Database: The Chinese Academy of Sciences Institute of Automation (CASIA V1.0) [26] iris database is considered to test the algorithm which consist of 756 eye images from 108 persons i.e., 7 eye image per individual.

B. Iris Biometric Technology: Figure1 shows the block diagram of iris biometric technology.

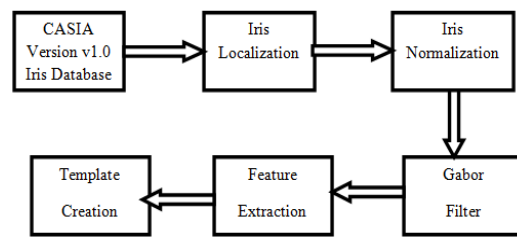


Figure 1: Iris Biometric Technology

All iris images are undergone with the localization and normalization of the iris in a minimum bounded isothetic rectangle (MBIR) format. The MBIR images are processed to obtain rectangular iris templates of size 120x200. The Canny edge detector is used to find the edge map of the eye image and Hough transform is used to identify the inner and outer boundaries of the iris. The boundaries are utilized to isolate the iris region from the original eye image. Gabor filter extraction is used to extract the features from iris template.

B. Watermark Embedding Process: The watermarking methodology of using hybrid format of the two robust techniques, that is discrete wavelet transform (DWT) and singular value decomposition (SVD) has been employed here. Figure2 shows watermark embedding process.

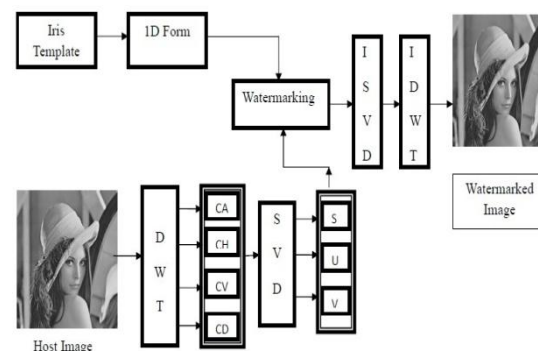


Figure 2: Watermark Embedding Process

The host image is applied with the single level decomposition Haar wavelet to obtain the four set of coefficients CA, CH, CV and CD. SVD is applied on each subbands, to obtain the two orthogonal matrices U and V and the set of Eigen values in S. For the band being CX (here as the same operation is repeated for the approximate band, that is, CA, horizontal band, that is, CH, vertical band, that is, CV and diagonal band, that is, CD the iterative method

is referred as CX, that is, CA/CH/CV/CD) the operation is as in the following equation

$$CX = U \times S \times V^T, CX = CA/CH/CV/CD \quad \dots 1$$

The iris biometric watermark is embedded in the eigen value matrix S to obtain S\*. Then SVD is again applied on the S\* matrix to obtain S<sub>1</sub>, U<sub>1</sub> and V<sub>1</sub>. Here too S<sub>1</sub> is the Eigen value matrix of S\*, whereas U<sub>1</sub> and V<sub>1</sub> are the orthogonal matrices. Now the orthogonal matrices of first SVD operation, that is. U and V are combined with the Eigen values of the second SVD operation that is S<sub>1</sub> to obtain the sub band for watermarked image that is CW.

$$U \times S_1 \times V^T = CW, CW = CA_w/CH_w/CV_w/CD_w \quad \dots 2$$

These operations applied on all the four sub bands, generate the four sub bands watermarked image. Similarly, the watermarked image is generated on application of IDWT on CA<sub>w</sub>, CH<sub>w</sub>, CV<sub>w</sub> and CD<sub>w</sub>.

### C. Watermark Extraction Process

For the extraction of the watermark from the stego image, the reverse of the above scheme is employed. Figure3 shows watermark extraction process.

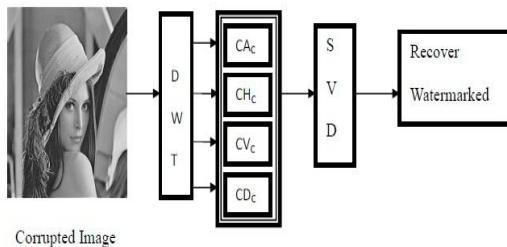


Figure 3: Watermark Extraction Process

Here the corrupted version of the watermarked image is considered to be received. Similar to the embedding process, the haar wavelet transform of the image is taken to obtain the corrupted image's sub bands CA<sub>c</sub>, CH<sub>c</sub>, CV<sub>c</sub>, and CD<sub>c</sub>. The image is decomposed back to its respective coefficients as well. Then on each respective sub band pair of corrupted image, the SVD is applied to obtain U<sub>c</sub>, S<sub>c</sub> and V<sub>c</sub>.

$$CX_D = CA_D/CH_D/CV_D/CD_D \quad \dots 3$$

Watermark template is recovered. This recovered watermark is compare with all the templates from standard database. If the features of recovered template are matches with the features of any of the template from standard database then person

identification is done. Based on this biometric watermark the person identification or detection of the user id of the subscriber is obtained. For matching Hamming distance is used.

### III. PERFORMANCE PARAMETERS

The performance parameters such as MSE, PSNR, NC, FAR and FRR are calculated to check the authenticity of system. These parameters are explained in following subsections.

#### Hamming Distance

HD is calculated as the sum of disagreeing bits over the total number of bits in the bit pattern, n. The equation is shown below,

$$HD = \frac{1}{n} \sum_{i=1}^n A_i + B_i$$

Where, n is the vector length and

A<sub>i</sub> and B<sub>i</sub> are the i<sup>th</sup> component of the template and sample vector.

#### Mean Square Error (MSE)

The Mean Square Error (MSE) measures the square of errors. The MSE represents the cumulative squared error between the reconstructed image and the original image.

$$MSE = \frac{1}{mn} \left( \sum_{i=0}^{m-1} \sum_{j=1}^{n-1} (I(i, j) - R(i, j))^2 \right)$$

Where, I and R can be interpreted as input and reconstructed images respectively. m and n defines number of pixel in vertical and horizontal dimension of images I and R.

#### Peak Signal to Noise Ratio (PSNR)

The Peak Signal-To-Noise Ratio (PSNR) represents a measure of the peak error. PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. Following formula shows PSNR is most easily defined via the mean squared error (MSE).

$$PSNR = 10 \log_{10} (255 \times 255 / MSE)$$

In case of ideal condition, if noise is zero, then MSE=0 and PSNR=∞.

#### False Acceptance Rate

The False Accept Rate, also known as a Type I1 error, measures the number of times an unauthorized user is accepted and therefore wrongly admitted to the protected system thus enabling a security breach and it can be calculated as

$$FAR = \frac{\text{Number of false acceptance}}{\text{Number of imposter verification}}$$

**False Rejection Rate**

The False Reject Rate, also known as a Type I error, measures the number of times an authorized user is wrongly refused access to the protected system. It is defined as the probability that the system fails to detect a match between the input pattern and a matching template in the database.

$$FRR = \frac{\text{Number of False Rejection}}{\text{Number of Enrollee Verification}}$$

**Normalized Cross Correlation (NC)**

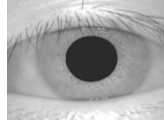

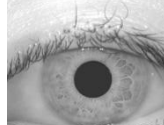

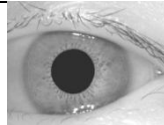
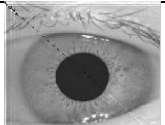
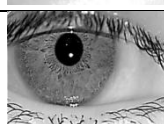

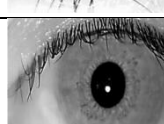

It is a measure used to evaluate the similarity between the embedded and the extracted watermarks. It is given by,



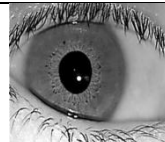

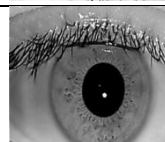
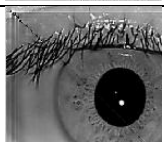
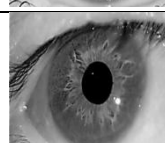
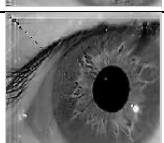
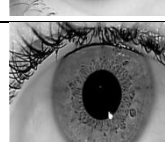

$$V_{NCC} = \frac{\sum_{i=1}^N \sum_{j=1}^N I_0(i,j)I_E(i,j)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N I_0^2(i,j)} \times \sqrt{\sum_{i=1}^N \sum_{j=1}^N I_E^2(i,j)}}$$

Where,  $I_0$  and  $I_E$  denote original and extracted binary watermarks.

**IV. RESULTS AND DISCUSSION**

The watermarked template and extracted template are mapped in terms of calculating Hamming distances. Table 1 shows the authenticity.

Sample Image	Extracted Image	Results
		Person 1 is authenticated
		Person 2 is authenticated
		Person 3 is authenticated
		Person 4 is authenticated
		Person 5 is authenticated

		Person 6 is authenticated
		Person 7 is authenticated
		Person 8 is authenticated
		Person 9 is authenticated
		Person10 is authenticated

Depending on the Hamming Distance we identify the correct person.

In the another experiment, 10 iris images from CASIA database are tested for two attacks to calculate the performance parameters MSE, PSNR, NC, Acceptance count and Rejection count. Table 2 shows values of PSNR, NC, MSE, Acceptance count and Rejection count for compression 20 attack.

Sample Image	PSNR	NC	MSE	Acceptance Count	Rejection Count
Image 1	61.74	0.96	0.221	10	0
Image 2	62.95	0.97	0.167		
Image 3	60.62	0.96	0.233		
Image 4	60.51	0.92	0.397		
Image 5	63.26	0.93	0.269		
Image 6	61.79	0.94	0.281		
Image 7	61.24	0.89	0.419		
Image 8	61.24	0.89	0.340		
Image 9	60.85	0.91	0.351		
Image10	62.90	0.88	0.357		

Table 3 shows values of PSNR, NC, MSE, Acceptance count and Rejection count for Noise 20 attack.

Sample Image	PSNR	NC	MSE	Acceptance Count	Rejection Count
Image 1	60.74	0.96	0.220	9	1
Image 2	61.39	0.97	0.166		
Image 3	59.73	0.96	0.237		
Image 4	60.08	0.91	0.421		
Image 5	62.20	0.93	0.270		
Image 6	60.91	0.94	0.285		
Image 7	60.85	0.89	0.433		
Image 8	60.63	0.89	0.343		
Image 9	60.21	0.91	0.352		
Image10	61.99	0.88	0.358		

#### V. CONCLUSION

Now a day, Security is one of the major concerns. Multimedia documents need to be protected from unauthenticated user so biometric watermarking system is used. Here in this system a non-blind approach of integrating the highly secure iris biometric will be integrated with the image watermarking algorithm to enhance multimedia security of data. Moreover the integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. From all these values, it is clear that the proposed system is performed very well for Compression attack but for Noise 20 attack 90% accuracy is achieved. If NC = 1 then the embedded watermark and the extracted watermark are same. Generally the value of NC>0.7500 is accepted as reasonable watermark extraction. Here we get NC values nearly equal to 1 that means embedded watermark is perfectly equal to extracted watermark.

#### ACKNOWLEDGMENT

I would like to thank Dr. P. M. Mahajan for valuable guidance at every step in making this paper. He motivated me and boosted my confidence and I must admit that work would not have been accomplished with his guidance and encouragement.

#### REFERENCES

1. D. Khannah and Dr. gobi, " survey on biometric based digital water- marking technique and

- applications, Global journal of computer science and technology, vol. 13, issue. 8, pp. 22-27, 2013.
2. Rimmi K Patel, "A Review on Watermarking Techniques for Biometric Security, IJARESM, pp. 1-6, 2012.
3. C.Karthikeyan and D.Selvamani , " Multimodal Biometric Watermarking Techniques: A Review, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 10, pp. 12542-12546, October 2014.
4. S.Sanderson and J.H.Erbetta, " Authentication for Secure Environments Based on Iris Scanning Technology, pp. 1-8. 2009.
5. Richard P. Wildes, " Iris Recognition: An Emerging Biometric Technology, proceedings of the IEEE, VOL. 85, NO. 9, pp. 1348-1363, September 1997.
6. Ion Marqus, Manuel Graa, " Image security and biometrics: A review, Grupo de Inteligencia Computacional, UPV/EHU [www.ehu.es/ccwintco](http://www.ehu.es/ccwintco)
7. Ruizhen Liu and Tieniu Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transactions on Multimedia, Vol. 4, No. 1, March 2002, pp. 121-128.
8. Stephane G. Mallat, " A Theory For Multiresolution Signal Decomposition: The Wavelet Representation, IEEE Transactions On Pattern Analysis And Machine Intelligence. Vol 11 . No. 7. July 1989. Pp. 674-693.
9. Rajesh M. Bodade, Dr. Sanjay N. Talbar, " Iris Recognition Using Rota-tional Complex Wavelet Filters: A Novel Approach, 2008 IEEE, 658-686.
10. N.G. Kingsbury, "The dual-tree complex wavelet transform: A new technique for shift invariance and directional filters, Proc. 8th IEEE DSP Workshop, Utah, Aug. 912, 1998, paper no. 86-20.
11. Peng Yao, Jun Li, Xueyi Ye, Zhenquan Zhuang, Bin Li, "Iris Recognition Algorithm Using Modified Log-Gabor Filters, The 18th International Conference on Pattern Recognition (ICPR'06), computer society, IEEE, 2006.
12. R. P. Wildes J. C. Asmuth G. L. Green S. C. Hsu R. J. Kolczynski J. R. Matey S. E. McBride, " A System for Automated Iris Recognition, 1994 IEEE, pages 121-128.

13. W. W. Boles and B. Boashash. "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE transactions on signal processing, vol. 46, no. 4, pages no- 185-198, April 1998.
14. D. M. Monro and D. Zhang, "Effective Human Iris Code with Low Complexity", Department of Electronic and Electrical Engineering, University of Bath, BA2 7AU, UK, 2005 IEEE.
15. J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 15, No. 11, PP. 1148-1161, 1993.
16. L. Ma, T. Tan, etc, "Efficient Iris Recognition by Characterizing Key Local Variations, IEEE Trans. on Image Processing, Vol. 13, PP. 739-750, 2004.
17. S. Rakshit and D. M. Monro, "An Effect of Sampling and Compression On Human Iris Verification", ICASSP 2006, IEEE, pp 237-340.
18. S. Majumder, T. S. Das, V. H. Mankar and S. K. Sarkar, "SVD and Error Control Coding based Digital Image Watermarking, International Conference on Advances in Computing, Control, and Telecommunication Technologies, computer society, IEEE, 2009, pp. 60-63.
19. Swanirbhar Majumder, Kharibam Jilenkumari Devi and Subir Kumar Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking, The Institution of Engineering and Technology 2013, Vol. 2, Iss. 1, pp. 2127.
20. Mrs.D.Mathivadhani, Dr.C.Meena, "Biometric Based Authentication Using Wavelets and Visual Cryptography", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, IEEE, pp 291-295.
21. S. Priyalakshmi and Sumathy Eswaran, "Robust and Secured Image Authentication System by Watermarking and Iris Biometric, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015, pp. 32-36.
22. Farinaz Dehestani Kolagar and Seyed Mohammad Jalal Rastegar Fatemi, "Steganography Of Fingerprint Images By Using Discrete Wavelet Transform, Volume- 4 Issue- 3, pp. 367-376, 2015.
23. De-song WANG, Jian-ping LI and Xiao-yang WEN, "Biometric Image Integrity Authentication Based on SVD and Fragile Watermarking, Congress on Image and Signal Processing, computer society, IEEE, pp. 679-608, 2008.
24. M. Saikia, S. Majumder, T. S. Das, Md. A. Hussain and S. K. Sarkar, "Coded Fingerprinting based Watermarking to Resist Collusion Attacks and Trace Colluders, International Conference on Advances in Computer Engineering, Computer society, IEEE, pp. 120-124, 2010.
25. Abdullah MAM, Dlay SS, Woo WL. Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform. In: 10th International Conference on Computer Vision Theory and Applications (VISAPP 2015). 2015, Berlin, Germany: INSTICC.
26. <http://www.sinobiometrics.com>, CASIA Iris Image Database.