Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 926170, 6 pages
http://dx.doi.org/10.1155/2014/926170

Research Article

Novel Iris Biometric Watermarking Based on Singular Value Decomposition and Discrete Cosine Transform

Jinyu Lu,[1] Tao Qu,[2] and Hamid Reza Karimi[3]

[1] *College of Engineering, Bohai University, Jinzhou 121013, China*
[2] *School of Electronics & Information Engineering, University of Technology Liaoning, Jinzhou, China*
[3] *Department of Engineering, Faculty of Engineering and Science, The University of Agder, 4898 Grimstad, Norway*

Correspondence should be addressed to Jinyu Lu; 156241142@qq.com

Received 5 December 2013; Accepted 27 December 2013; Published 16 February 2014

Academic Editor: Weichao Sun

A novel iris biometric watermarking scheme is proposed focusing on iris recognition instead of the traditional watermark for increasing the security of the digital products. The preprocess of iris image is to be done firstly, which generates the iris biometric template from person's eye images. And then the templates are to be on discrete cosine transform; the value of the discrete cosine is encoded to BCH error control coding. The host image is divided into four areas equally correspondingly. The BCH codes are embedded in the singular values of each host image's coefficients which are obtained through discrete cosine transform (DCT). Numerical results reveal that proposed method can extract the watermark effectively and illustrate its security and robustness.

1. Introduction

With the internet age coming, amount of digital products have swarmed into our living. Especially the digital products are inevitable for being copy-free. Therefore, the security of these products is presented over the past few decades. A typical solution is the digital watermarking technology which has been widely applied to information security, such as copyright protection and authentication. Watermarking can be classified into visible and invisible. Visible watermarking is attacked even more than invisible because visible watermarking is disclosed [1]. In contrast, invisible watermarking is more prevalent. Invisible watermarking could be done in the spatial domain or in the transform domain according to human visual system (HVS). However, transform-domain-based watermarking techniques present advantages in terms of perceptibility and robustness more than the spatial domain, so more researchers pay attention to the transform domain. Researchers frequently used the transform domain including the Fourier transform, discrete cosine transform (DCT), discrete wavelet transform (DWT), and many more.

In biometrics feature recognition, iris has become focus and emphasis which has unique, stability, be-collected, non-invasion, and so forth as an important characteristic of authentication. Daugman has made many contributions to iris-based biometrics [2, 3]. Wildes et al. have proposed an automated iris recognition [4]. Wildes et al. [4, 5], Boles and Boashash [6] have obtained some research on the iris recognition. More and more research institutes and companies have been added to the field of iris recognition [7, 8]; iris-based authentication technology is paid attention to by academia and business. A lot of standard databases have been generated by various institutes to work in this field [9, 10]. Lots of organizations are focusing on the issue, such as Chinese Academy of Sciences-Institute of Automation (CASIA) [11], Lion's Eye Institute (LEI) [12], Universities of Bath, and Carnegie Mellon University, and we use the database from University of Bath. Similar method is discussed in [13–20].

To sum up, we focus on the iris biometric database, a novel iris biometric watermarking based on singular value decomposition (SVD), and DCT is proposed.

The preprocess of iris image is to be done firstly, which generates the iris biometric template from person's eye images. And then the templates are to be on discrete cosine transform; the value of the discrete cosine is converted to BCH-based coding. The host image is divided into four areas equally correspondingly. The DCT coefficients of each area

are applied with the SVD [21, 22]. The DCT coefficients of each area are modified by the singular vectors and the BCH-based error control coding watermark to embed the watermark image. Embedding intensities depends on the key. The algorithm is robust under popular attacks.

2. Iris Image Technology Normalization and Coding

We use the database of eye images from University of Bath. In addition to iris, there are pupil, sclera, and eyelid in any eye image. It is necessary to normalize to remove these adverse factors from eye image prior to coding. We apply a minimum bounded isothetic rectangle (MBIR) format to eye image for eliminating these factors. Thus, we obtain rectangular iris templates which are normalized to a size of 120×200 pixels by MBIR format [23, 24]. The normalized 120 × 200 iris image is applied with column-wise, 1D DCT and retaining of DC value of each column, to obtain a 1 × 200 set of pixels [23, 25, 26]. Then, these 1 × 200 DC values are encoded to binary string, which is 8 × 200 bits format with BCH-based error control coding (Figure 1).

3. Watermarking Methodology

Discrete cosine transform is correlated with Fourier transform, which is similar to the discrete Fourier transform and only use real parts. 2D DCT transformation is commonly used in video compression conversion. In the compression process, the image is divided into many small pieces of 8 × 8 format. A signal $x(i, j)$ is converted into frequency domain as follows:

$$y(k,m) = \alpha(k)\cdot\alpha(m)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left\{x(i,j)\times\cos\left[\frac{(2i+1)k\pi}{2N}\right]\cdot\cos\left[\frac{(2j+1)m\pi}{2N}\right]\right\},$$
$$x(i,j) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left\{\alpha(k)\cdot\alpha(m)\,y(k,m)\times\cos\left[\frac{(2i+1)k\pi}{2N}\right]\times\cos\left[\frac{(2j+1)m\pi}{2N}\right]\right\}, \quad (1)$$

where $N = 8$. Then the watermark-embedding process is discussed in the following steps.

Step 1. The host image I is divided into four blocks equally I^j, which block is applied with DCT I_D^j, $j = 1, 2, 3, 4$.

SVD is an important matrix factorization in linear algebra which has some important application in signal processing, statistics, and other fields.

Suppose M is a $m \times m$ matrix, the elements of which all belong to K domain, that is, real domain or complex domain. Thus, it exists a decomposition such that:

$$M = U\sum V^T, \quad (2)$$

where U is $m \times m$ unitary matrix and V^T is the conjugate transpose of V which also is $m\times m$ unitary matrix. We choose special orthonormal bases: $v_1, \ldots, v_m$ for the row space and $u_1, \ldots, u_m$ for the column space. $\sum$ is positive semidefinite matrix of $m \times m$ and is the singular value of M:

$$\sum = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_m),$$
$$M = U_1\lambda_1V_1 + \cdots + U_m\lambda_mV_m. \quad (3)$$

Step 2. I_D^j is implemented by SVD for each block:

$$I_D^j = U_D^j S_D^j {V_D^j}^T,$$
$$U_D^j S_D^j {V_D^j}^T = \operatorname{SVD}\left(I_D^j\right), \quad j = 1, 2, 3, 4. \quad (4)$$

Step 3. Iris image is normalized and encoded to binary string. Here iris image is converted to 8 × 200 bits binary, which is divided into four sections equally and each section is 400 bits binary. The 400 bits binary change into 403 bits added with 3 zero values at the end of the 400 bits. The 403 bits binary is converted to BCH(511,403), where $n = 511$, $k = 403$, and $t = 12$. The watermark consists of these four sections.

Step 4. Watermark is embedded into the singular values of the DCT-transformed host image on each block:

$$S_D'^j = S_D^j + \alpha I_w. \quad (5)$$

Step 5. The DCT coefficients of watermarked image are modified in each block:

$$I_D'^j = U_D'^j S_D'^j {V_D'^j}^T. \quad (6)$$

Step 6. The watermarked image is performed inverse DCT (IDCT) on $I_D'^j$.

For illustrating the watermark embedded process, the description figure is presented as shown in Figure 2.

For the watermark-extraction process, we consider that the received image is corrupted version of the watermarked image. And the description of the watermark extraction process is presented in Figure 3.

Step 1. In this step of the extraction process, the corrupted image I'' is divided into four areas I''^j ($j = 1, 2, 3, 4$) equally.

Step 2. I''^j is applied with DCT:

$$I_D''^j = \operatorname{DCT}\left(I''^j\right). \quad (7)$$

Step 3. SVD operation is implemented on $I_D''^j$:

$$I_D''^j = U_D'^j S_D''^j {V_D'^j}^T,$$
$$U_D'^j S_D''^j {V_D'^j}^T = SVD\left(I_D''^j\right). \quad (8)$$

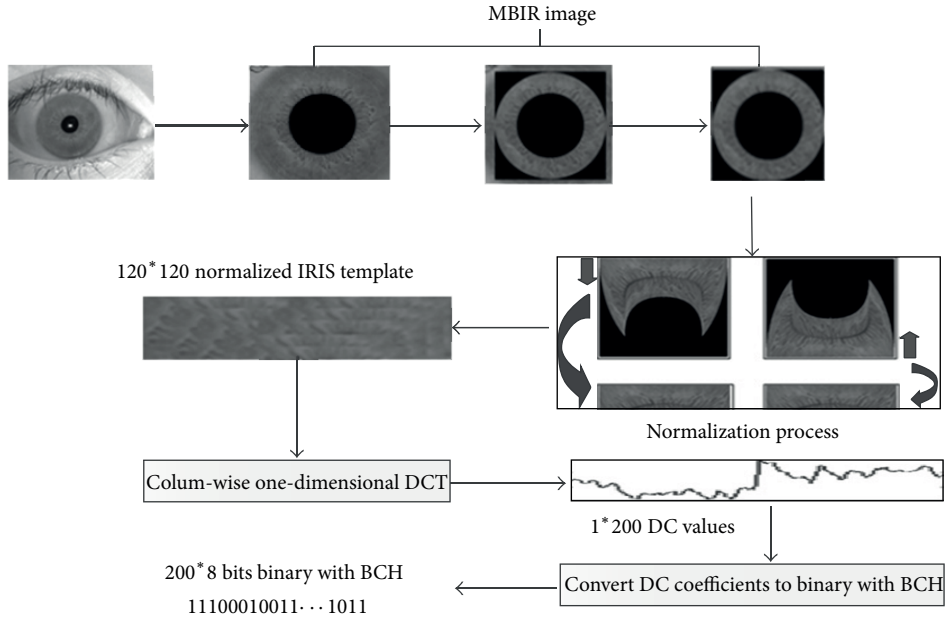

Figure 1: Iris biometric normalization and coding.

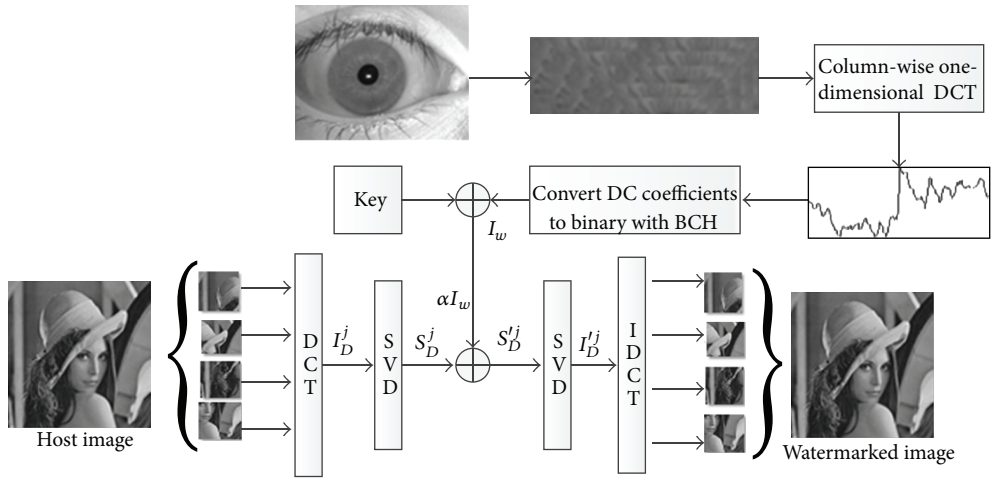

Figure 2: Watermark embedded process.

Step 4. Watermark is hidden in the singular value of $I_D''^j$, so watermark $I_w'^j$ is expressed by the following:

$$I_w'^j = \frac{1}{\alpha_j}\left(U^T\left(I_D''^j - I_D^j\right)V\right). \tag{9}$$

Step 5. $I_w'^j$ is divided into four sections equally; then, each section is processed error correction decoding, as $I_w'^j$ is binary BCH coding. The result of the decoding is that I_w^{*j} is 1600 bits binary format.

Step 6. Perform mod 2 operation on I_w^{*j}:

$$A_{ij} = I_w^{*i} \oplus I_w^{*j}, \quad i, j = 1, 2, 3, 4, \tag{10}$$

where $A_{ii} = \mathbf{0}$, $A_{ij} = A_{ji}$, $A_{ij} = \{a_1^{ij}, a_2^{ij}, \ldots, a_{1600}^{ij}\}$, and A_{ij} is vector.

Step 7. Do a summation of the elements in A_{ij}:

$$M_{ij} = \sum_{r=1}^{1600} a_r^{ij}, \quad i \neq j. \tag{11}$$

Step 8. Take the minimum of M_{ij} as I_w^*:

$$I_w^* = I_w^{*i} \text{ or } I_w^{*j}. \tag{12}$$

Step 9. This is done conversion of the binary format I_w^* into the DC values.

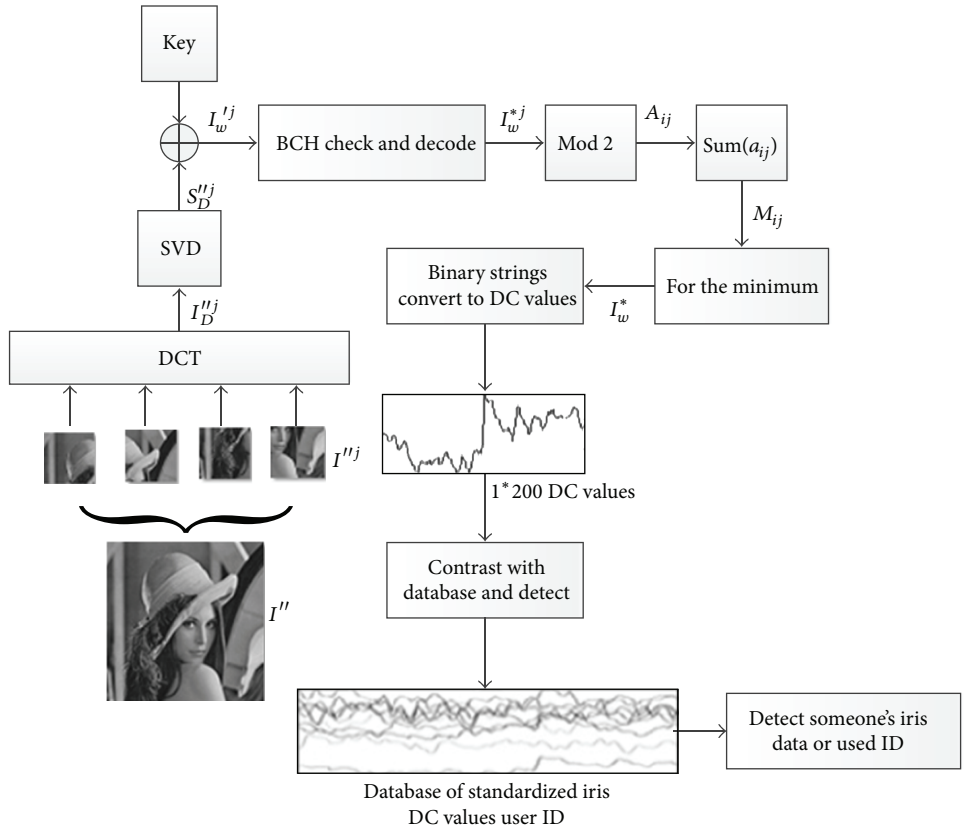

Figure 3: Watermark extraction process.

Step 10. The obtained set of DC coefficients is contrasted with the standard sets of DC coefficients stored for each person and judged to belong to who in the database.

4. Experiment Results and Discussion

Because the iris biometric has the superiority of security, imperceptibility, the iris biometric is employed to realize embed watermark. Via the conclusions discussed in [27], the DC coefficients of different persons' iris, which can be seen to be noncorrelated, has a non-self-similar characteristic as shown in [27]. However, the variation of DC coefficients of the same iris biometric has a self-similar characteristic as in [27] in diversification condition. In terms of iris characteristics, the DC coefficients of iris biometric are used as a watermark.

The detected watermark is a binary string in our proposed scheme, so the detected watermark is divided into two types of situation. One type of situation is that the detected watermark could match up with someone's iris biometric in the database, so it is the identification of the biometric. The embedded watermark and the detected watermark belong to the same iris, that is, correct detection, or the embedded watermark and the detected watermark do not belong to the same iris, that is, false acceptance. Another type of situation is that the detected watermark could not match up with anyone's iris biometric in the database, so it is false rejection. In the above types, we only pay attention to correct detection, for it is significant to identify the detected watermark. According to Figures 1–3, the proposed scheme and the algorithm [23] are all viewed as digital communication system, it has greatly raised the correct-detection probability. Thus it is hard to measure the performance by traditional methods such as PSNR and ROC curve, it can be to measure the performance by the algorithm [23].

In [27], there are 77 different attacks. In their results of experiment, both the identification 67 of the 77 attacks which has greater than 90% of correct detection and the identification 71 of the 77 attacks which has greater than 85% of correct detection have been successful. This algorithm [27] displays robustness when receiving most attacks by detection and identification except the "copy" attack. Some attacks like "scaling," "MAP," "up-down sampling," and "bending" attacks are partially sustained. In this paper, the proposed algorithm almost has a good performance with the different attacks. There are 70 different attacks; the identification 60 of the 70 attacks which has greater than 95% of correct detection, the identification 61 of the 70 attacks which has greater than 90% of correct detection, and the identification 66 of the 70 attacks which has greater than 85% of correct detection have been successful, all shown in Table 1.

Table 1: Major attack-wise total number of correct detections, false rejections, and false acceptances for $70 \times 400 = 28000$ tests.

	M	NM	W (%)			CD (%)			FR (%)			FA (%)			T
			>95	>90	>85	95	90	85	95	90	85	95	90	85	
1	Aspect ratio	30	29	29	30	11776	11835	11862	216	158	132	8	7	6	12000
2	Crop	6	5	5	6	2371	2380	2389	25	18	10	4	2	1	2400
3	JPEG	7	6	6	7	2724	2756	2767	73	42	31	3	2	2	2800
4	Scale	6	4	4	5	1905	1987	2093	448	382	285	47	31	22	2400
5	MAP	6	4	5	5	1396	1548	2173	935	810	200	69	42	27	2400
6	Up-down sample	4	2	2	3	1251	1385	1452	335	204	139	14	11	9	1600
7	Remodulation	4	4	4	4	1574	1582	1591	26	18	9	0	0	0	1600
8	Filtering	3	3	3	3	1189	1192	1197	10	7	3	1	1	0	1200
9	Bending	2	1	1	1	462	481	490	338	319	310	1	0	0	800
10	Copy	2	2	2	2	781	788	795	19	12	5	0	0	0	800
T		70	60	61	66	25429	25934	26809	2425	1970	1124	147	96	67	28000

Note. M: expresses major attack type, NM: expresses number of subattacks, W: expresses watermark detection cases, CD: expresses correct detection, F: expresses false rejection, FA: expresses false acceptance, and T: expresses total.

5. Conclusion

In this paper, the DC coefficients of the same iris biometric have a self-similar characteristic to reduce complexity of implementation. BCH(511,403) codes have a 12 bits error-correction function. It has largely improved the correct-detection probability of extracted watermark in comparison with traditional watermark. Furthermore, four extracted watermarks are compared one by one so that the best one can be selected. This process also improves the correct-detection probability. A series of experiments have been conducted to validate the performance of the proposed SVD and DCT. The experimental results show that the proposed scheme has a more superior performance than the other methods under different kinds of attacks. The proposed algorithm based on SVD and DCT has robustness and imperceptibility.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This present work was supported partially by the Polish-Norwegian Research Programme (Project no. Pol-Nor/200957/47/2013). The authors highly appreciate the above financial supports.

References

[1] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121–128, 2002.

[2] S. Sanderson and J. H. Erbetta, "Authentication for secure environments based on Iris scanning technology," *IEE Colloquium*, no. 18, pp. 53–59, 2000.

[3] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[4] R. P. Wildes, J. C. Asmuth, G. L. Green et al., "System for automated iris recognition," in *Proceedings of the 2nd IEEE Workshop on Applications of Computer Vision*, pp. 121–128, December 1994.

[5] R. P. Wildes, "Iris recognition: an emerging biometrie technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[6] 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, pp. 1185–1188, 1998.

[7] A. K. Jain, R. M. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*, Springer, 1999.

[8] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[9] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[10] R. P. Wildes, J. C. Asmuth, G. L. Green et al., "A machine-vision system for iris recognition," *Machine Vision and Applications*, vol. 9, no. 1, pp. 1–8, 1996.

[11] L. Masek, *Recognition of Human Iris Patterns for Biometric Identification [M.S. thesis]*, University of Western, Australia, 2003.

[12] C. Barry and N. Ritter, *Database of 120 Grayscale Eye Images [M.S. thesis]*, Lions Eye Institute, Perth Western Australia.

[13] S. Yin, S. X. Dinga, A. H. A. Sari et al., "Data-driven monitoring for stochastic systems and its application on batch process," *International Journal of Systems Science*, vol. 44, no. 7, pp. 1366–1376, 2013.

[14] S. Yin, H. Luo, and S. Ding, *Real-Time Implementation of Fault-Tolerant Control Systems With Performance Optimization*, 2013.

[15] S. Yin, X. Yang, and H. R. Karimi, "Data-driven adaptive observer for fault diagnosis," *Mathematical Problems in Engineering*, vol. 2012, Article ID 832836, 21 pages, 2012.

[16] B. Xiao, Q. Hu, and M. I. Friswell, "Robust fault tolerant control for spacecraft attitude stabilization under actuator faults and bounded disturbance," *Journal of Dynamic Systems, Measurement and Control, Transactions of the ASME*, vol. 133, no. 5, Article ID 051006, 2011.

[17] S. Yin, S. X. Ding et al., "A comparison study of basic data-driven fault diagnosis and process monitoring methods on the benchmark Tennessee Eastman process," *Journal of Process Control*, vol. 22, no. 9, pp. 1567–1581, 2012.

[18] S. Yin, G. Wang, and H. R. Karimi, "Data-drivendesign of robust fault detection system for wind turbines," *Mechatronics*. In press.

[19] W. Sun, H. Gao Sr., and O. Kaynak, "Finite frequency H_∞ control for vehicle active suspension systems," *IEEE Transactions on Control Systems Technology*, vol. 19, no. 2, pp. 416–422, 2011.

[20] W. Sun, Z. Zhao, and H. Gao, *Saturated Adaptive Robust Control For Active Suspension Systems*, 2013.

[21] S. G. Mallat, "Theory for multiresolution signal decomposition: the wavelet representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 7, pp. 674–693, 1989.

[22] K. Loukhaoukha, J.-Y. Chouinard, and M. H. Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization," *Journal of Information Hiding and Multimedia Signal Processing*, no. 4, pp. 303–319, 2011.

[23] R. Kalita, S. Majumder, and M. A. Hussain, "Multidimensional multimetric novel and simple techniques for iris recognition system," *International Journal of Recent Trends in Engineering*, vol. 3, no. 3, pp. 161–166, 2010.

[24] S. Majumder, A. D. Singh, and M. Mishra, "A GUI based Iris authentication system for secured access," in *Proceedings of the International Conference on Systemics, Cybernetics and Informatics (ICSCI '09)*, under Pentagram Research, Hyderabad, India, 2009.

[25] D. M. Monro and D. Zhang, "An effective human Iris code with low complexity," in *Proceedings of the IEEE International Conference Image Processing*, vol. 3, pp. 277–280, 2005.

[26] Q. Zhao, *Advanced Information Security Technology: Watermarking and Biometrics*, ACM-HK Student Research and Day, 2009.

[27] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," *IET Biometrics*, vol. 2, no. 1, pp. 21–27, 2013.