Published in Biometrics
Received on 12th September 2012
Revised on 4th December 2012
Accepted on 22nd January 2013
doi: 10.1049/iet-bmt.2012.0052

ISSN 2047-4938

# Singular value decomposition and wavelet-based iris biometric watermarking

*Swanirbhar Majumder[1], Kharibam Jilenkumari Devi[1], Subir Kumar Sarkar[2]*

*[1]Department of ECE, NERIST (Deemed University), Arunachal Pradesh, India*
*[2]Department of ETCE, Jadavpur University, West Bengal, India*
*E-mail: swanirbhar@ieee.org*

**Abstract:** These days, with technological advancement, it is very easy for miscreants to produce illegal multimedia data copies. Various techniques of copyright protection of free data are being developed daily. Digital watermarking is one such technique, where digital embedding of the copyright information/watermark into the data to be protected. The two major ways of doing so are spatial domain and the robust transform domain. In this study, method for watermarking of digital images, with biometric data is presented. The usage of biometric instead of the traditional watermark increases the security of the image data. The biometric used here is iris. After the retinal scan, it is the most unique biometric. In terms of user friendliness in extracting the biometric, it comes after fingerprint and facial scan. The iris biometric template is generated from subject's eye images. The discrete cosine values of templates are extracted through discrete cosine transform and converted to binary code. This binary code is embedded in the singular values of the host image's coefficients generated through wavelet transform. The original image is thus firstly applied with the discrete wavelet transform followed up by the singular value decomposition of the subband coefficients. The algorithm has been tested with popular attacks for analysis of false recognition and rejection of subjects.

## 1 Introduction

The World Wide Web or WWW phenomena since the late part of the 20th century have demonstrated the commercial potential of free multimedia resources through the digital networks. Multi National Companies (MNCs), for their commercial interests, needs to use the digital networks to offer digital media [1]. However, they also have a necessity of protecting their ownership rights. So here along with cryptography and other alternatives, digital watermarking too, steps in as one of the popular way to accomplish the same. Owing to the advanced copying/replicating tools available to duplicate and modify those multimedia data, security is a major concern. Thus protecting digital multimedia data is very important. There are many types of digital information and data like digital images, audio and video. Watermarking can be either visible or invisible. Visible watermark is used in images and videos but they tend to spoil the beauty and moreover the position of the watermark is disclosed to the attackers in this case [2]. This led to the popularity of the invisible watermarking, where the position of the watermark is not open to the public. Invisible watermarking may be done either in the spatial domain or the transform domain. The method presented here is of the transform domain variant because of the extra robustness of the same [3].

There are various techniques of implementing transform domain watermarking like Fourier transform, discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) and many more. Here DWT- and SVD-based hybrid transform domain has been used. This is because the multiresolution property of DWT increases the imperceptibility, whereas SVD aids in improving the robustness of the scheme [4, 5]. Unlike the traditional methods of using an image or a random signal as a watermark, here the authentication information used as watermark is the iris biometric data of the user. It is used as the user id in this case, similar to various methods that use a logo as watermark. A biometric is based on the concept of 'something – you-are', so it increases the security criteria many folds in comparison to the traditional watermarking methods [6].

Biometrics like iris, retinal scan, fingerprint scan, hand geometry, facial scan and so on carries the unique biological information about the user. Retinal scan is the most secure of these but it is not very user friendly, whereas facial scan, finger print and hand geometry are the most user-friendly but not as much secure as iris or retinal scan [7]. Iris biometric gives an optimised option of user-friendly as well as secure biometric. This is because an iris image of a person can be collected from a distance of couple of meters unlike retinal scan, finger print or hand geometry [8]. Moreover unlike fingerprint once a person is dead his pupils stop dilating so the iris scan of a dead person does not match with a live one. Whereas in comparison to facial scan iris biometrics of twins are not same, and neither do they change with age like the human face [9].

## 2 Iris biometric recognition

Daugman was one of the pioneers in the field of iris-based biometrics [10, 11] and holds patents [12] in this field as well. Wildes *et al.* [13, 14], Boles and Boashash [15], Lim *et al.* [16], Noh *et al.* [17], Monro and Zhang [18] and Rakshit and Monro [19] followed up the trend with their respective good work. A lot of standard databases have been generated by various institutes to work in this field. Starting from Chinese Academy of Sciences – Institute of Automation (CASIA), Lion's Eye Institute (LEI), Universities of Bath, Carnegie Mellon University, and many more including institutes, even our very own Indian Institute of Technology, Delhi, in India [20, 21].

Here the database used is of University of Bath. The idea here is about identifying the host image and authenticating it through the biometric to avoid colluders. So a very simple methodology has been used to normalise the biometric data in a robust, useable format so that the complexity of the biometrics along with watermarking technology is reduced [18, 19].

## 3 Watermarking and iris biometric technology

The idea of implementing both the technologies, that is, biometrics and watermarking has been done in two ways. The first, watermarking a biometric data, which is used as a host with a watermark, for protection of the integrity of the biometric data to enhance the security [22]. Whereas the second is where the watermark is a biometric and is used for the authentication of the host image. Here the work is of the second type [23]. Previously, researchers have used mainly fingerprint and face for this second type of watermarking a host image with a biometric for its protection [24, 25].

The method used is very simple taken from our previous work [26]. However, out of the various multi-metric techniques proposed, the easiest and the one having lowest complexity, as well as time constraint with significant identification is proposed. The method can be implemented either row-wise or column-wise, in one-dimensional (1D) DCT of the intensities. This is done to obtain the DC coefficients after DCT to give a 1D sequence of DC values for the 2D greyscale iris biometric intensity image. This 1D biometric data here is used as the watermark. The scheme employed here is similar on the lines of hybrid transform [27].

The DCT of a row of the iris matrix is defined as

$$X_i^n(k, l) = w(k) \sum_{l=1}^{M} x(n, l) \cos \frac{(2l-1)(k-1)}{2M}, \quad k = 1, 2, .....M \tag{1}$$

where $x\ (n,\ l)$ is $l$th sample of the signal in the $n$th row of the $i$th iris image, $M$ is the column size, and $w(k) = \sqrt{1/M}$ for $k = 1$ and $w(k) = \sqrt{2/M}$ for $2 \le k \le M$.

The steps employed, as in Fig. 1, to obtain the iris biometric in 1D watermark format is as under:

The database of eye images obtained from university of bath is taken. There are 20 images of each eye (both left and right) of 20 different persons. Thus we have a database of $2 \times 20 \times 20$ images of which only the left eye images are taken, that is, 400 images [18, 19].

These 400 images are undergone with the normalisation and extraction of the iris in a minimum bounded isothetic rectangle (MBIR) format.

The MBIR-ed images are processed to obtain rectangular iris templates, normalised to a size of $120 \times 200$ pixels each [26, 28].

The normalised $120 \times 200$ iris images are applied with column-wise, 1D DCT and retaining of DC value of each column, to obtain a $1 \times 200$ set of pixels.

These 200 DC values are converted to binary, that is, $200 \times 8$ bit format and added with CRC-based error control coding.

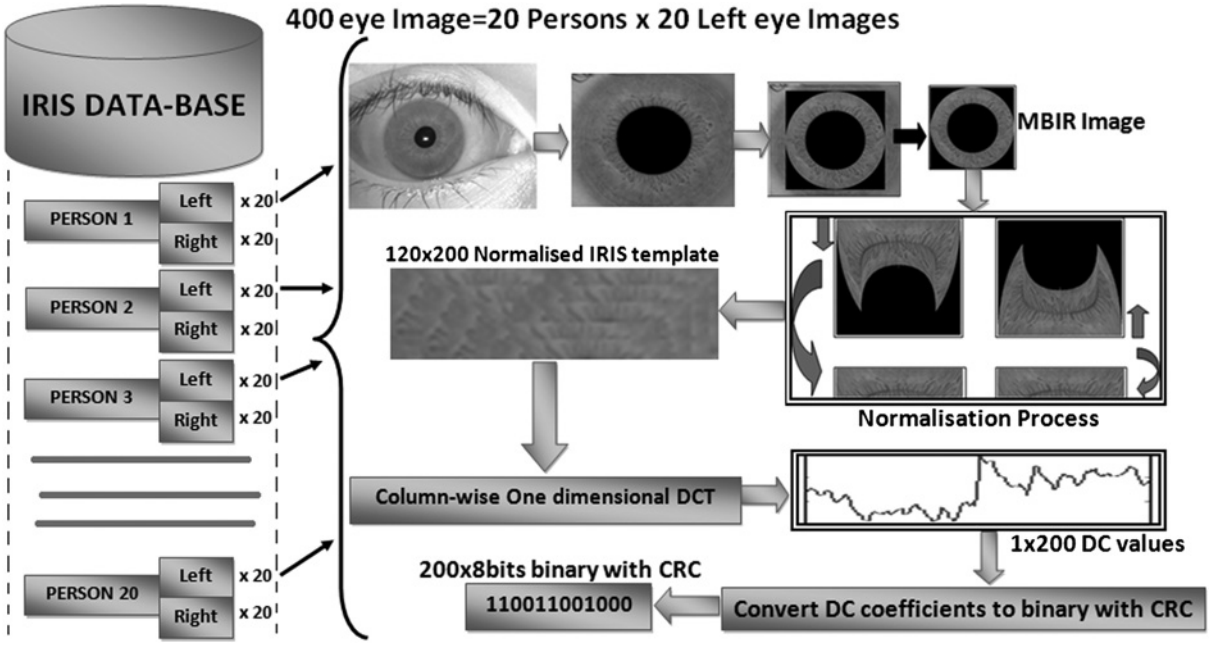


**Fig. 1** *Iris biometric technology implemented*




doi: 10.1049/iet-bmt.2012.0052

## 4 Watermarking methodology

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 [29, 30]. The host image is applied with the single level DWT using Daubechies ($N = 6$) wavelet to obtain the four set of coefficients CA, CH, CV and CD. This is followed up by SVD operation on each of them on similar lines, to obtain the two orthogonal matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ and the set of eigen values in $\boldsymbol{S}$. 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

$$\mathrm{CX} = \boldsymbol{U} \times \boldsymbol{S} \times \boldsymbol{V}^{\mathrm{T}}, \quad \mathrm{CX} = \mathrm{CA/CH/CV/CD} \tag{2}$$

The iris biometric watermark is embedded in the eigen value matrix $\boldsymbol{S}$ to obtain $\boldsymbol{S}^*$ with $\mathrm{CRC}_{200}$ being the CRC-based 200 DC values of the iris template in binary, as in (3). The CRC used is MATLABs inbuilt CRC-16 cyclic redundancy check codes [31, 32]. This $\mathrm{CRC}_{200}$ is divided by the threshold KEY; this is to reduce the payload of the embedded watermark (Fig. 2). Then SVD is again applied on the $\boldsymbol{S}^*$ matrix to obtain $\boldsymbol{S}_1$, $\boldsymbol{U}_1$ and $\boldsymbol{V}_1$. Here too $\boldsymbol{S}_1$ is the Eigen value matrix

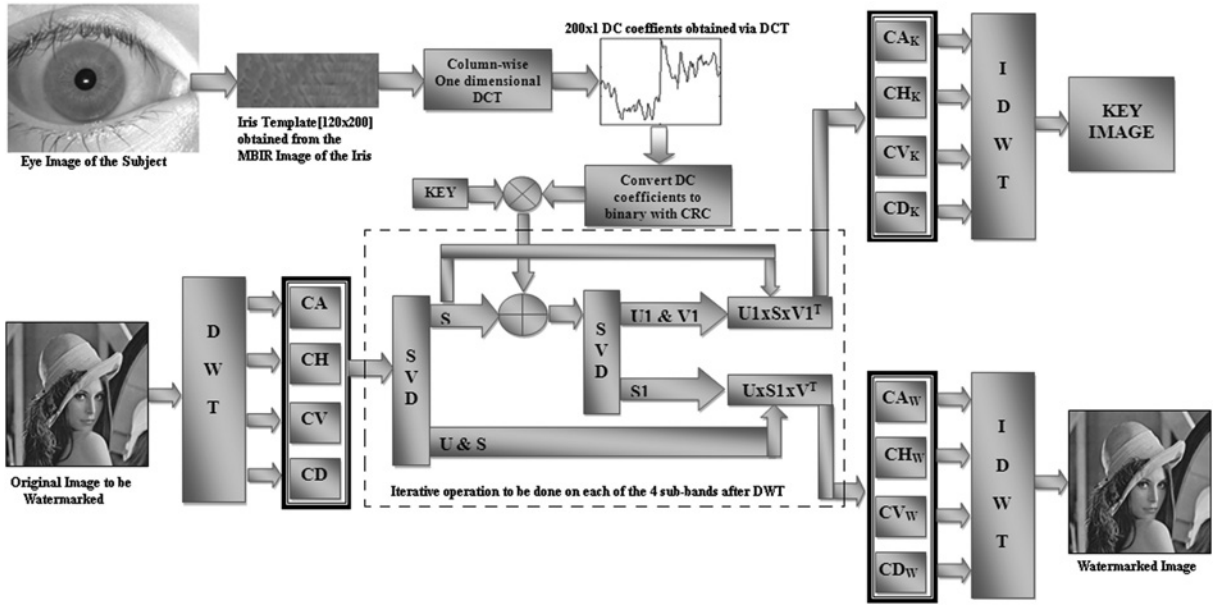


**Fig. 2** *Iris biometric based image watermarking algorithm*

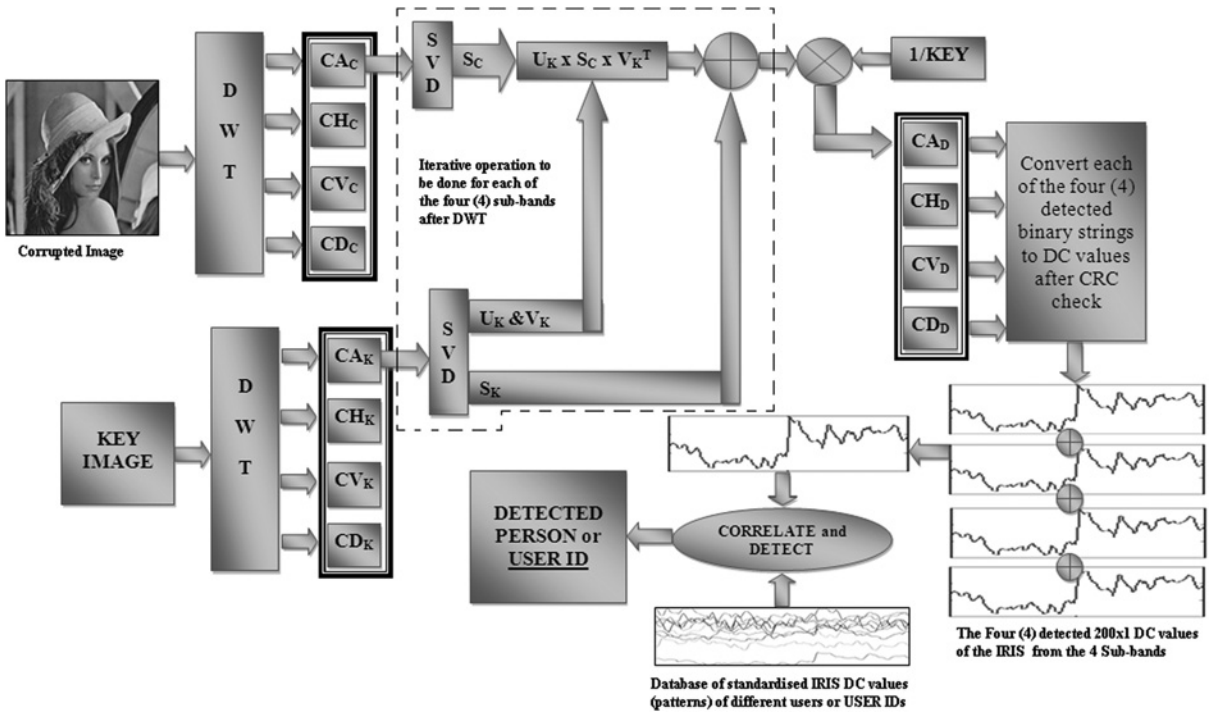


**Fig. 3** *Watermark extraction and biometric identification algorithm*

of $S*$, whereas $U_1$ and $V_1$ are the orthogonal matrices. The $CRC_{200}$ data are added to the modified Eigen value matrix in a linearised way

$$S* = S_1 + \mathrm{CRC}_{200}/\mathrm{KEY} = U_1 \times S \times V_1^{\mathrm{T}} \quad (3)$$

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 $S_1$ to obtained the subband for watermarked image, that is CW. The rest, that is $U_1$ and $V_1$ are combined with the Eigen values of the first SVD operation, $S$ to obtain CK, the subband for the key image. Though they could be kept as key matrices instead it is preferred to keep them as 'key image' as this would require less memory in place of keeping them as key matrices. In case there are no memory constraints they can be kept as key matrices and be used whereas extraction of the watermark (Fig. 3). Here the word 'key image' refers to the image required during the extraction procedure along with the corrupted image

$$U \times S_1 \times V^{\mathrm{T}} = \mathrm{CW}, \quad \mathrm{CW} = \mathrm{CA}_W/\mathrm{CH}_W/\mathrm{CV}_W/\mathrm{CD}_W \quad (4)$$

$$U_1 \times S \times V_1^{\mathrm{T}} = \mathrm{CK}, \quad \mathrm{CK} = \mathrm{CA}_K/\mathrm{CH}_K/\mathrm{CV}_K/\mathrm{CD}_K \quad (5)$$

These operations applied on all the four subbands, generate the four subbands for both key image and watermarked image. Then on application of the inverse discrete wavelet transform (IDWT) on the $CA_K$, $CH_K$, $CV_K$ and $CD_K$ generates the key image. Similarly, the watermarked image is generated on application of IDWT on $CA_W$, $CH_W$, $CV_W$ and $CD_W$.

For the extraction of the watermark from the stego image, the reverse of the above scheme is employed. Here the corrupted version of the watermarked image is considered to be received. Similar to the embedding process, the DWT of the image is taken to obtain the corrupted image's subbands $CA_C$, $CH_C$, $CV_C$, and $CD_C$. The image is decomposed back to its respective coefficients as well. Then on each respective subband pair of corrupted image and key image, the SVD is applied to obtain $U_C$, $S_C$, $V_C$, $U_K$, $S_K$, and $V_K$, respectively. The Eigen values of the stego image, $S_C$ are combined with the respective orthogonal matrices $U_K$ and $V_K$ of the key image to generate the stego subband matrix $D$ as in (6). The Eigen values of the key image $S_K$ are then subtracted from the matrix $D$ to obtain the watermark coefficients $CX_D$ for that particular subband after normalisation with the threshold named KEY, as in (7).

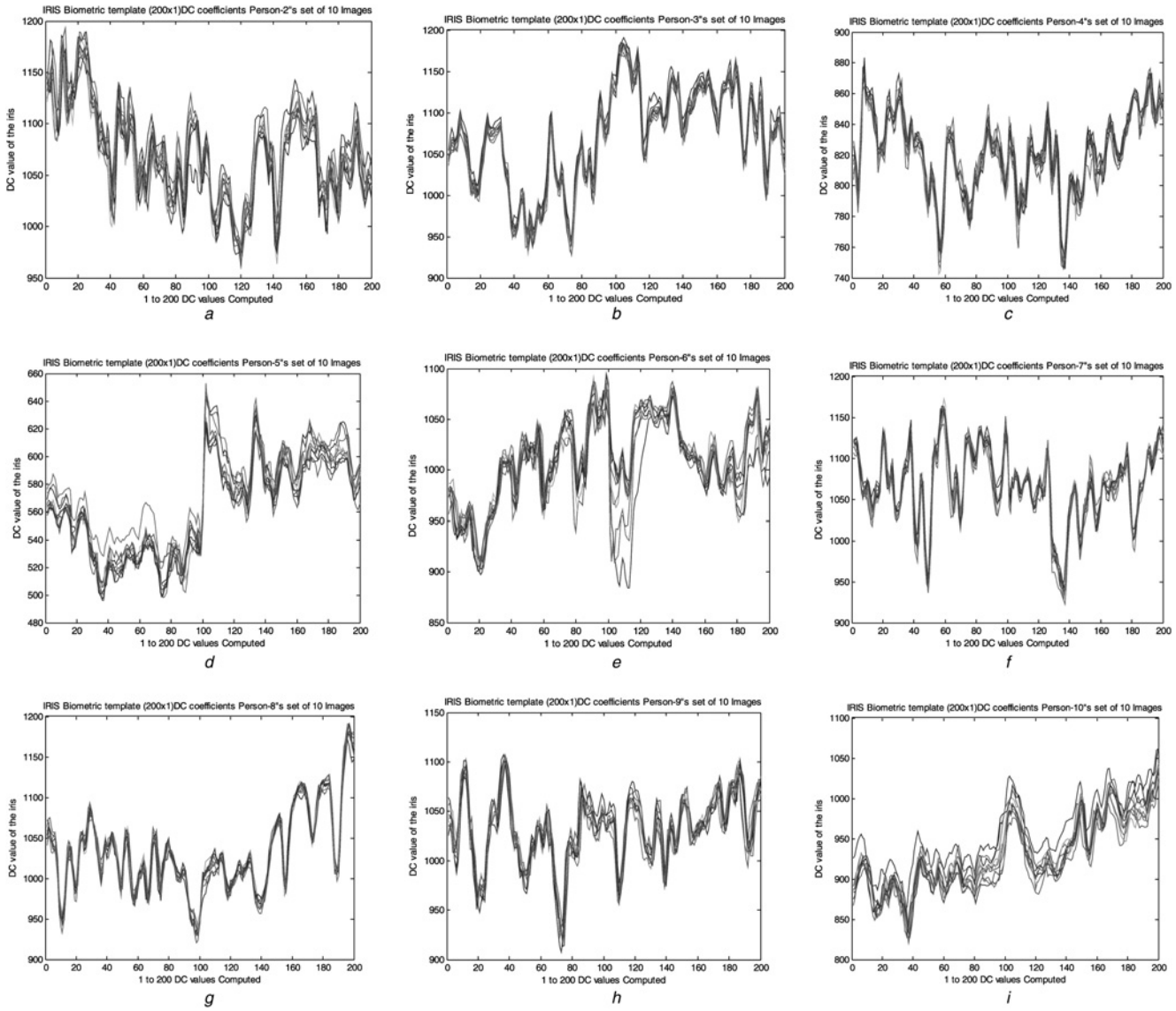


**Fig. 4** *DC coefficients of ten images for nine different persons' a, b, c, d, e, f, g, h and i*




doi: 10.1049/iet-bmt.2012.0052

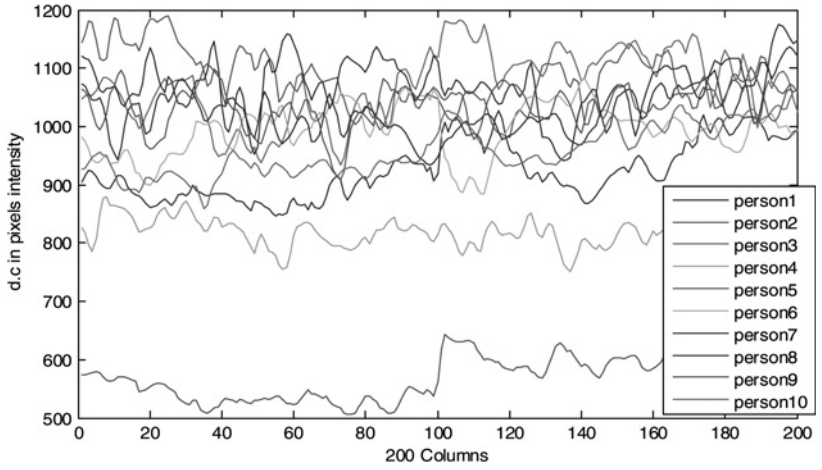


**Fig. 5** *DC coefficients of ten different persons' single randomly chosen image*

This KEY was the multiplying factor applied to CRC DC coefficients to reduce the intensity in the embedding process.

$$\boldsymbol{D} = \boldsymbol{U}_K \times \boldsymbol{S}_C \times \boldsymbol{V}_K^{\mathrm{T}} \tag{6}$$

$$\begin{aligned} \mathrm{CX}_D &= \left(1/\mathrm{KEY}\right) \times \left(\boldsymbol{D} - \boldsymbol{S}_K\right), \\ \mathrm{CX}_D &= \mathrm{CA}_D/\mathrm{CH}_D/\mathrm{CV}_D/\mathrm{CD}_D \end{aligned} \tag{7}$$

So from the obtained watermark coefficients $\mathrm{CA}_D$, $\mathrm{CV}_D$, $\mathrm{CH}_D$, and $\mathrm{CD}_D$ the four sets of DC values of the iris biometric is obtained. This is done by firstly removing the CRC error control coding redundant bits, followed by conversion of the binary data to pixel intensities of the DC values. From the set of the four set of DC values detected from the four wavelet subbands a normalised set of DC coefficient is obtained. This obtained set of DC coefficient is correlated with the standard sets of DC coefficient stored for each person for detection, authentication and identification of the biometric watermark. Based on this biometric watermark the person identification or detection of the user id of the subscriber is obtained. This is done using the self-similarity patterns as per our previous work [26]. There it was found that the DC coefficients follow a particular self-similarity pattern for every particular eye. Even the left and right eye of any particular person follows a different set of pattern.

## 5 Results and discussion

The watermark to be embedded in the image for security, here is an iris biometric. As only the DC values are embedded

**Table 1** Number of attacks sustained by the Watermarking algorithm for 90 and 85% tolerance in maximum cases

| Sl no | Major attack type | Different sub attacks | No of sub-attacks | Watermark detection cases for more than | |
|---|---|---|---|---|---|
| | | | | 90% | 85% |
| 1 | aspect ratio | ratios used = 1, 3, 4, 5, 6 | 35 | 34 | 34 |
| 2 | crop | with C factor (quality factor for JPEG/bits per pixel for wavelet) = 0.4, 0.5, 0.6, 0.8, 1.5, 3.5, 8 and *x* and *y* scales varying in between 0.8, 0.9, 1.0, 1.1 and 1.2 | 7 | 7 | 7 |
| 3 | JPEG | cropping with C factor (quality factor for JPEG/bits per pixel for wavelet) = 0.4, 0.5, 0.6, 0.8, 1.5, 3.5, 8 | 7 | 7 | 7 |
| 4 | scale | compression with C factor (quality factor for JPEG/bits per pixel for wavelet) = 50, 60, 75, 80, 85, 90 and 100 | 6 | 4 | 5 |
| 5 | MAP | scaling with C factor (quality factor for JPEG/bits per pixel for wavelet) = 1.5, 3.5 and 8 with each having scales 0.9 and 1.1 | 6 | 3 | 5 |
| 6 | up–down sample | mapping with C factor (quality factor for JPEG/bits per pixel for wavelet) = 100 for Wiener, hard and soft threshold with each having windows 3 and 5 | 4 | 2 | 3 |
| 7 | re-modulation | with down sampling 0.75 and 0.5 and up sampling for 1.33, 1.2, 1.3 and 1.9 | 4 | 4 | 4 |
| 8 | filtering | denoising and remodulation attack with basic remodulation attack and basic remodulation attack assuming a correlated watermark with prediction window size 3 and 5 | 3 | 3 | 3 |
| 9 | bending | Gaussian filter of sizes 3 and 5 and sharpening filter of size 3 | 2 | 1 | 1 |
| 10 | wavelet | approximates the random bending attack with stirmark with C factor (quality factor for JPEG/bits per pixel for wavelet) = 3.5 and 8 | 2 | 2 | 2 |
| 11 | copy | wavelet compression with C factor (quality factor for JPEG/bits per pixel for wavelet) = 1.5, 3.5 and 8 | 1 | 0 | 0 |
| total | | | 77 | 67 | 71 |

**Table 2** Major attack-wise total number of correct detections, false rejections and false acceptances for 77 × 400 = 30800 tests

| Sl no. | Major attack type | No of sub-attacks | Watermark detection cases for more than | | Correct detection | | False rejection | | False acceptance | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 90% | 85% | 90% | 85% | 90% | 85% | 90% | 85% | |
| 1 | aspect ratio | 35 | 34 | 34 | 13720 | 13834 | 271 | 159 | 9 | 7 | 14000 |
| 2 | crop | 7 | 7 | 7 | 2754 | 2766 | 41 | 32 | 5 | 2 | 2800 |
| 3 | JPEG | 7 | 7 | 7 | 2766 | 2771 | 32 | 27 | 2 | 2 | 2800 |
| 4 | scale | 6 | 4 | 5 | 1823 | 2120 | 539 | 261 | 38 | 19 | 2400 |
| 5 | MAP | 6 | 3 | 5 | 1429 | 2213 | 923 | 158 | 48 | 29 | 2400 |
| 6 | up–down sample | 4 | 2 | 3 | 1107 | 1345 | 482 | 245 | 11 | 10 | 1600 |
| 7 | re-modulation | 4 | 4 | 4 | 1587 | 1592 | 13 | 8 | 0 | 0 | 1600 |
| 8 | filtering | 3 | 3 | 3 | 1193 | 1193 | 7 | 7 | 0 | 0 | 1200 |
| 9 | bending | 2 | 1 | 1 | 512 | 547 | 286 | 253 | 2 | 0 | 800 |
| 10 | wavelet | 2 | 2 | 2 | 784 | 784 | 16 | 16 | 0 | 0 | 800 |
| 11 | copy | 1 | 0 | 0 | 3 | 6 | 397 | 394 | 0 | 0 | 400 |
| total | | 77 | 67 | 71 | 27678 | 29171 | 3007 | 1560 | 115 | 69 | 30800 |

along with a reduced threshold [dividing by KEY as in (3)], the PSNR of the image is high. In spite of four times embedding of the iris biometric a PSNR around 53 dB is achieved. Therefore there must be watermark detection after attacks and the identification of the biometric as well. The variation of DC coefficients of each of the nine different persons', ten images have a self-similar characteristics with a high inter correlation as shown in Fig. 4. The DC coefficients are seen to follow a particular type of pattern out here, based on which they can be differentiated. But if the DC coefficients of different persons' iris for any one image are plotted together they can be seen to be non-correlated. This can be seen from the non-self-similar features as in Fig. 5.

This is because of the need to justify the usage of the biometric as watermark as well as showing of robust security measures. For the sake of watermark identification the tests are performed, as per the Checkmark 1.2 developed by Shelby Pereira of University of Geneva, Vision Group [29]. This has been mainly estimated on their 'Logo' application which has 77 different subattacks. The total number of cases analysed for the 20 images of 20 different persons' single eye is $20 \times 20 = 400$. So including all the 77 different subattacks, total number of cases is $77 \times 400 = 30\,800$.

In case of above 90% correct detection and identification 67 of the 77 attacks have been successful and for above 85% we have 71 of the 77 cases. Here by 85% success and 90% success the percentage of allowable bit pattern difference is represented. These are tabulated in Table 1. The details of the 30 800 cases for correct detection, false detection and false rejection for both the cases are tabulated in Table 2.

Thus based on these two tables it can be seen that on an average maximum attacks are sustained by the algorithm except for the 'copy' attack. Whereas for some attacks like 'scaling', 'MAP', 'up-down sampling' and 'bending' attacks are partially sustained.

## 6 Conclusion

Here in this paper a non-blind approach of integrating the highly secure iris biometric has been integrated with the image watermarking algorithm to enhance multimedia security of data. The algorithm here for the biometric generation has been kept very simple to reduce complexity of implementation. Moreover the integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. Thus this scheme provides a secure-robust-imperceptible watermarking technology in total.

## 7 Acknowledgment

The authors acknowledge TEQIP Phase-II of Jadavpur University, for the work presented in this paper.

## 8 References

1 Katzenbeisser, S., Petitcolas, F.A.P.: 'Information hiding techniques for steganography and digital watermarking' (Artech house, Computer security series, 2000), pp. 15–23, 97–109
2 Liu, R., Tan, T.: 'A SVD-based watermarking scheme for protecting rightful ownership', *IEEE Trans. Multimedia*, 2002, **4**, pp. 121–128
3 Johnson, N.F., Duric, Z., Jajodia, S.: 'Information hiding, steganography' (Kluwer Academic Publisher, 2003), pp. 15–29
4 Mallat, S.: 'A theory for multiresolution signal decomposition: the wavelet representation', *IEEE Trans. Pattern Anal. Mach. Intell.*, 1989, **11**, pp. 674–693
5 Zhu, X., Zhao, J., Xu, H.: 'A digital watermarking algorithm and implementation based on improved SVD watermarking-attacks and counter measures'. Proc. 18th IEEE Computer Society Int. Conf. Pattern Recognition (ICPR'06)
6 Masek L.: 'Recognition of human iris patterns for biometric identification'. Bachelor thesis for School of Computer Science and Software Engineering, The University of Western Australia, 2003
7 Bertillon, A.: 'la couleur de iris' (Revue Scientifique, France, 1985)
8 Bodade, R.M., Talbar, S.N., Ojha, S.K.: 'Iris recognition using rotational complex wavelet filters' (IEEE, 2008)
9 Yao, P., Li, J., Ye, X., Zhang, Z., Li, B.: 'Iris recognition algorithm using modified log-gabor filters'. IEEE 18th Int. Conf. Pattern Recognition, 2006
10 Sanderson, S., Erbetta, J.: 'Authentication for secure environments based on iris scanning technology', *IEE Colloq. Vis. Biometrics*, 2000, **2000**, pp. 811–817 DOI:10.1049/ic:20000468
11 Daugman, J.: 'How iris recognition works'. Proc. of 2002 Int. Conf. on Image Processing, 2002, vol. 1
12 Daugman, J.: 'Biometric personal identification system based on iris analysis'. United States Patent, Patent Number: 5,291,560, 1994
13 Wildes, R., Asmuth, J., Green, G., *et al*: 'A system for automated iris recognition'. Proc. IEEE Workshop on Applications of Computer Vision, Sarasota, FL, 1994, pp. 121–128
14 Wildes, R.: 'Iris recognition: an emerging biometric technology', *Proc. IEEE*, 1997, **85**, (9), pp. 1348–1363
15 Boles, W., Boashash, B.: 'A human identification technique using images of the iris and wavelet transform', *IEEE Trans. Signal Process.*, 1998, **46**, (4), pp. 1185–1188
16 Lim, S., Lee, K., Byeon, O., Kim, T.: 'Efficient iris recognition through improvement of feature vector and classifier', *ETRI J.*, 2001, **23**, (2) (Korea)

17 Noh, S., Pae, K., Lee, C., Kim, J.: 'Multiresolution independent component analysis for iris identification'. 2002 Int. Technical Conf. Circuits/Systems, Computers and Communications, Phuket, Thailand, 2002

18 Monro, D.M., Zhang, D.: 'An effective human Iris code with low complexity'. Proc. IEEE Int. Conf. on Image Processing, September 2005, vol. 3, pp. 277–280

19 Rakshit, S., Monro, D.M.: 'Effects of sampling and compression on human Iris verification'. Proc. IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, May 2006, vol. 2, no. II, pp. 337–340

20 Chinese Academy of Sciences – Institute of Automation. Database of 756 Greyscale Eye Images. Available at http://www.sinobiometrics.com Version 1.0, 2003

21 Barry, C., Ritter, N.: 'Database of 120 Greyscale eye images' (Lions Eye Institute, Perth Western Australia), 1999

22 Dong, J., Tan, T.: 'Effects of watermarking on iris recognition performance'. Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008, ICARCV 2008, p. 1156.

23 Majumder, S., Dutta, T.S.: 'Watermarking of data using biometrics', in: Dr. Bhattacharyya, S., Dutta, P., (Eds.), 'Handbook of research on computational intelligence for engineering, science and business' (IGI Global, 2030) pp. 623 (Chapter 24)

24 Zhao, Q.: 'Advanced information security technology: watermarking and biometrics' (ACM-HK Student Research and Day, 2009)

25 Varbanov, G., Blagoev, P.: 'An improving model watermarking with iris biometric code'. Int. Conf. on Computer Systems and Technologies – CompSysTech'07, 2007

26 Kalita, R., Majumder, S., Hussain, M.A.: 'Multidimensional multimetric novel and simple techniques for iris recognition system', *Int. J. Recent Trends Eng.*, 2010, **3**, (3), pp. 161–166, ACADEMY Publishers, Finland

27 Sverdlovsk, A., Dexter, S., Eskicioglu, A.M.: 'Robust SVD DCT based watermarking for copyright protection', *EEE Trans. Image Process.*, 2001, **10**, (5), pp. 72–73

28 Majumder, S., Singh, A.D., Mishra, M.: 'A GUI based Iris authentication system for secured access'. Int. Conf. Systemics, Cybernetics, Informatics (ICSCI-2009) under Pentagram Research, Hyderabad held, 7–10 January 2009, CC2.6 pp. 147–151

29 Majumder, S., Das, T.S., Mankar, V.H., Sarkar, S.K.: 'SVD and error control coding based digital image watermarking'. ID 61, Int. Conf. on Advances in Computing, Control and Telecommunication Technologies'2009(ACT 2009), organized by ACEEE and published by IEEE Computer Society, held at Trivendrum, India, pp. 60–63.

30 Saikia, M., Majumder, S., Das, T.S., Hussain, Md.A., Sarkar, S.K.: 'Coded fingerprinting based watermarking to resist collusion attacks and trace colluders'. Proc. Int. Conf. in Advances in Computer Engineering (ACE-2010), pp. 120–124 doi: 110.1109/ACE.2010.36 published by IEEE CS DL on 21 and 22 June 2010, in Bangalore

31 Sklar, B.: 'Digital communications: fundamentals and applications' (Prentice-Hall, Englewood Cliffs, NJ, 1988)

32 Wicker, S.B.: 'Error control systems for digital communication and storage' (Prentice-Hall, Upper Saddle River, NJ, 1995)