Singular value decomposition and wavelet-based iris biometric watermarking

Swanirbhar Majumder¹, Kharibam Jilenkumari Devi², Subir Kumar Sarkar²

¹Department of ECE, NERIST (Deemed University), Arunachal Pradesh, India
²Department 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 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

$$X_{m}^{n}(k, l) = w(k) \sum_{l=1}^{M} x(n, l) \cos \left(\frac{(2l-1)(k-1)}{2M}\right).$$

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

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

1. 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].

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

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

4. 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.

5. 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
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 $U$ 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

$$CX = U \times S \times V^T, \; CX = CA/CH/CV/CD$$  \hspace{1cm} (2)

The iris biometric watermark is embedded in the eigen value matrix $S$ to obtain $S^*$ with 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 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 $S^*$ matrix to obtain $S_1$, $U_1$ and $V_1$. Here too $S_1$ 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<sub>200</sub> data are added to the modified Eigen value matrix in a linearised way

$$S^* = S_1 + \text{CRC}_{200}/\text{KEY} = U_1 \times S \times V_1^T$$

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 obtain 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

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

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

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 $\text{CA}_K$, $\text{CH}_K$, $\text{CV}_K$ and $\text{CD}_K$ generates the key image. Similarly, the watermarked image is generated on application of IDWT on $\text{CA}_W$, $\text{CH}_W$, $\text{CV}_W$ and $\text{CD}_W$.

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 $\text{CA}_C$, $\text{CH}_C$, $\text{CV}_C$, and $\text{CD}_C$. 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 $\text{CX}_D$ 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
This KEY was the multiplying factor applied to CRC DC coefficients to reduce the intensity in the embedding process.

\[ D = U_K \times S_C \times V_T^T \]  
(6)

\[ C_X_D = \left( \frac{1}{\text{KEY}} \right) \times \left( D - S_K \right), \]

\[ C_X_D = \frac{C_{D_1}}{C_{D_2}}/\frac{C_{D_3}}{C_{D_4}} \]  
(7)

So from the obtained watermark coefficients \( C_{D_1}, C_{D_2}, C_{D_3}, \) and \( C_{D_4} \) 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

![DC coefficients of ten different persons' single randomly chosen image](image)

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

<table>
<thead>
<tr>
<th>Sl no</th>
<th>Major attack type</th>
<th>Different sub attacks</th>
<th>No of sub-attacks</th>
<th>Watermark detection cases for more than</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ratios used = 1, 3, 4, 5, 6</td>
<td>35</td>
<td>90%: 34, 85%: 34</td>
</tr>
<tr>
<td>1</td>
<td>aspect ratio</td>
<td>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</td>
<td>7</td>
<td>90%: 7, 85%: 7</td>
</tr>
<tr>
<td>2</td>
<td>crop</td>
<td>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</td>
<td>7</td>
<td>90%: 7, 85%: 7</td>
</tr>
<tr>
<td>3</td>
<td>JPEG</td>
<td>compression with C factor (quality factor for JPEG/bits per pixel for wavelet) = 50, 60, 75, 80, 85, 90 and 100</td>
<td>6</td>
<td>90%: 6, 85%: 6</td>
</tr>
<tr>
<td>4</td>
<td>scale</td>
<td>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</td>
<td>6</td>
<td>90%: 6, 85%: 6</td>
</tr>
<tr>
<td>5</td>
<td>MAP</td>
<td>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</td>
<td>4</td>
<td>90%: 4, 85%: 3</td>
</tr>
<tr>
<td>6</td>
<td>up-down sample</td>
<td>with down sampling 0.75 and 0.5 and up sampling for 1.33, 1.2, 1.3 and 1.9</td>
<td>4</td>
<td>90%: 4, 85%: 4</td>
</tr>
<tr>
<td>7</td>
<td>re-modulation</td>
<td>denoising and remodulation attack with basic remodulation attack and basic remodulation attack assuming a correlated watermark with prediction window size 3 and 5</td>
<td>3</td>
<td>90%: 3, 85%: 3</td>
</tr>
<tr>
<td>8</td>
<td>filtering</td>
<td>Gaussian filter of sizes 3 and 5 and sharpening filter of size 3</td>
<td>2</td>
<td>90%: 2, 85%: 2</td>
</tr>
<tr>
<td>9</td>
<td>bending</td>
<td>approximates the random bending attack with stirmark with C factor (quality factor for JPEG/bits per pixel for wavelet) = 3.5 and 8</td>
<td>2</td>
<td>90%: 2, 85%: 2</td>
</tr>
<tr>
<td>10</td>
<td>wavelet</td>
<td>wavelet compression with C factor (quality factor for JPEG/bits per pixel for wavelet) = 1.5, 3.5 and 8</td>
<td>1</td>
<td>90%: 1, 85%: 0</td>
</tr>
<tr>
<td>11</td>
<td>copy</td>
<td></td>
<td>77</td>
<td>90%: 77, 85%: 71</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sl no</th>
<th>Major attack type</th>
<th>Different sub attacks</th>
<th>No of sub-attacks</th>
<th>Watermark detection cases for more than</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>aspect ratio</td>
<td>ratios used = 1, 3, 4, 5, 6</td>
<td>35</td>
<td>90%: 34, 85%: 34</td>
</tr>
<tr>
<td>2</td>
<td>crop</td>
<td>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</td>
<td>7</td>
<td>90%: 7, 85%: 7</td>
</tr>
<tr>
<td>3</td>
<td>JPEG</td>
<td>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</td>
<td>7</td>
<td>90%: 7, 85%: 7</td>
</tr>
<tr>
<td>4</td>
<td>scale</td>
<td>compression with C factor (quality factor for JPEG/bits per pixel for wavelet) = 50, 60, 75, 80, 85, 90 and 100</td>
<td>6</td>
<td>90%: 6, 85%: 6</td>
</tr>
<tr>
<td>5</td>
<td>MAP</td>
<td>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</td>
<td>6</td>
<td>90%: 6, 85%: 6</td>
</tr>
<tr>
<td>6</td>
<td>up-down sample</td>
<td>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</td>
<td>4</td>
<td>90%: 4, 85%: 3</td>
</tr>
<tr>
<td>7</td>
<td>re-modulation</td>
<td>with down sampling 0.75 and 0.5 and up sampling for 1.33, 1.2, 1.3 and 1.9</td>
<td>4</td>
<td>90%: 4, 85%: 4</td>
</tr>
<tr>
<td>8</td>
<td>filtering</td>
<td>denoising and remodulation attack with basic remodulation attack and basic remodulation attack assuming a correlated watermark with prediction window size 3 and 5</td>
<td>3</td>
<td>90%: 3, 85%: 3</td>
</tr>
<tr>
<td>9</td>
<td>bending</td>
<td>Gaussian filter of sizes 3 and 5 and sharpening filter of size 3</td>
<td>2</td>
<td>90%: 2, 85%: 2</td>
</tr>
<tr>
<td>10</td>
<td>wavelet</td>
<td>approximates the random bending attack with stirmark with C factor (quality factor for JPEG/bits per pixel for wavelet) = 3.5 and 8</td>
<td>2</td>
<td>90%: 2, 85%: 2</td>
</tr>
<tr>
<td>11</td>
<td>copy</td>
<td>wavelet compression with C factor (quality factor for JPEG/bits per pixel for wavelet) = 1.5, 3.5 and 8</td>
<td>1</td>
<td>90%: 1, 85%: 0</td>
</tr>
<tr>
<td>total</td>
<td></td>
<td></td>
<td>77</td>
<td>90%: 77, 85%: 71</td>
</tr>
</tbody>
</table>
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 × 20 = 400. So including all the 77 different subattacks, total number of cases is 77 × 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


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


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


