IRIS RECOGNITION PERFORMANCE ENHANCEMENT
USING WEIGHTED MAJORITY VOTING

Sheikh Ziauddin, Matthew N. Dailey

Computer Science and Information Management
Asian Institute of Technology
P.O. Box 4, Klong Luang, Pathumthani 12120 Thailand.

ABSTRACT

Biometric authentication is a convenient and increasingly reliable way to prove one's identity. Iris scanning in particular is among the most accurate biometric authentication technologies currently available. However, despite their extremely high accuracy under ideal imaging conditions, existing iris recognition methods degrade when the iris images are noisy or the enrollment and verification imaging conditions are substantially different. To address this issue and enable iris recognition on less-than-ideal images, we introduce a weighted majority voting technique applicable to any biometric authentication system using bitwise comparison of enrollment-time and verification-time biometric templates. In a series of experiments with the CASIA iris database, we find that the method outperforms existing majority voting and reliable bit selection techniques. Our method is a simple and efficient means to improve upon the accuracy of existing iris recognition systems.

Index Terms— Biometrics, iris recognition, weighted majority voting

1. INTRODUCTION

Biometric authentication has proven to be a reliable way to verify a human's identity. The technology has certain advantages over more traditional password-, pin-, or hardware token-based human identification systems. First, biometric traits cannot easily be stolen, forged, or guessed. Second, there is no need to remember one's biometric traits. Third, biometrics are difficult to repudiate. Due to these benefits, biometric authentication systems are being deployed in many real-world applications. Current systems employ many different biometric traits, including fingerprints, iris images, face images, retinal scans, palmprints, and gait patterns.

Biometrics based on the *iris* are among the most accurate existing techniques for human identification and verification. Systems by Daugman [1], Wildes et al. [2], Boles et al. [3], and Zhu et al. [4] perform extremely well on the data sets they were designed for. However, the performance of any such system is highly dependent on the quality of the input iris images. As noise increases, any algorithm's performance will decrease. On noisy databases like UBIRIS [5] and CASIA [6], even the best known algorithms are unable to achieve an EER of 0 [7][8].

To mitigate the effect of noisy iris images, researchers have proposed a few techniques using multiple enrollment-time iris scans to
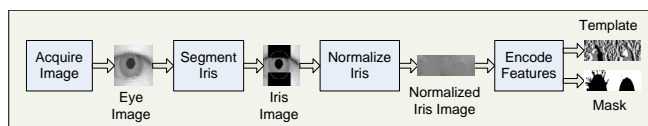
Fig. 1. Iris template generation process. The eye image is from CASIA version 1 [6].

improve verification performance. These approaches treat the iris template generation algorithm as a black box, so they do not depend on any particular algorithm. Davida et al. [9] present a *majority voting* technique to overcome the 10–20% bit error rates they observed between in enrollment- and verification-time iris templates. Their system acquires an odd number of scans at enrollment time and produces a "canonical" template vector that contains a 1 (or 0) wherever a majority of the corresponding bits in the original templates contain a 1 (or 0). Yang et al. [10] propose *reliable bit selection*. Their system acquires multiple scans (not necessarily an odd number) and computes the corresponding template vectors at enrollment time, then determines which bits are *identical* in every template. At verification time, the bits that were not identical (are not reliable) are ignored.

In this paper, we present a new scheme to enhance the performance of iris recognition systems. Rather than treating each bit equally (as in Davida et al.'s system) or completely ignoring bits that are not unanimous at enrollment time (as in Yang et al.'s system), we weight each bit according to its reliability at enrollment time. The result is a simple and efficient scheme that works with any iris template generation method and outperforms both majority voting and reliable bit selection on the CASIA [6] iris database.

2. IRIS RECOGNITION

2.1. Iris Template Generation

In an iris recognition system, the user presents his or her eye to an iris sensor, which images the user's iris and generates a template from this image. Most iris scanners use near infrared illumination with normal monochrome CMOS or CCD camera sensors that are sensitive to near infrared light.

After image acquisition, we use Masek and Kovesi's algorithm [11, 12] for iris template generation, which is based primarily on Daugman's methods [13]. Generating an iris template from a raw eye image involves three steps: iris segmentation, iris normalization, and iris feature encoding. Figure 1 shows the iris template generation process schematically.

The iris segmentation procedure segments the annular iris region from the entire eye image. First, it finds the circular inner and outer boundaries (the iris-pupil and iris-sclera boundaries) of the iris using a circular Hough transform. Then it marks the region of the annular iris ring that is not visible due to eyelids and eyelashes. The method uses a linear Hough transform to find the eyelids and a simple thresholding technique to find eyelashes covering the iris image.

The iris normalization procedure transforms the segmented iris region into a rectangular grid of 240×20 pixels using a polar-to-Cartesian transformation and bilinear interpolation. To minimize the effect on encoding of corrupted regions detected during segmentation, the method sets the intensity of corrupted regions to the neighborhood's mean intensity.

The feature encoding procedure encodes the normalized iris image as a binary string. At each pixel in the 240×20 image, it extracts information about local texture characteristics as described by convolution with a horizontal one-dimensional log-Gabor wavelet filter [14] whose real and imaginary components form a quadrature pair. The frequency response of a log-Gabor filter is

$$G(f) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right)$$

where f_0 is the base frequency and σ is the bandwidth of the filter. The method uses $f_0 = 0.056$ cycles/pixel (13.44 cycles/iris) and $\sigma = 0.5$.

Following Daugman [13], the method discards the amplitude of the complex-valued response and quantizes the phase so that only its quadrant in the complex plane is retained, using a two-bit Gray code. The result is a 9600-bit template ($240 \times 20 \times 2$), which is combined with the corrupted bit mask computed in the segmentation stage.

2.2. Iris Template Comparison

The most common metric for iris template comparison is the *Hamming* metric. The normalized Hamming distance between two binary strings is the number of positions in which the strings differ from each other, divided by the size of each string [13]:

$$HD(T, T') = \frac{1}{n}\sum_{i=1}^{n} t_i \oplus t_i' \qquad (1)$$

where T and T' represent the two templates to be matched and n is the size of iris template.

When information about masked (corrupted) bits is incorporated, we exclude bits in the template that are marked as corrupted by the corresponding mask:

$$HD(T, T', M, M') = \frac{\sum_{i=1}^{n}(t_i \oplus t_i') \wedge m_i \wedge m_i'}{\sum_{i=1}^{n} m_i \wedge m_i'} \qquad (2)$$

where T and T' represent the two templates to be matched and M and M' represent corresponding masks. $\wedge$ represents the bitwise AND operation.

3. PROPOSED SCHEME

At enrollment time, we obtain n images of the user's iris, where n is an odd integer. (In our experiments with CASIA, reported in Section 4, we use $n = 5$.) For each of the n scans, we generate a 9600-bit iris *base template*, as described in Section 2.1.

We then generate a single combined *final template* T containing the majority votes of the n base templates. A bit t_i in the final template contains a 1 if more than $n/2$ corresponding bits in the base templates are 1; otherwise it contains a 0.

In addition to T, we also generate a weight vector W that describes the reliability of the individual bits in the final template. We let the ith element w_i of W, corresponding to the ith element t_i of T, be the proportion of base templates containing t_i (the majority vote for the ith bit). A high value for w_i indicates that t_i is highly reliable, and a low value for w_i indicates that t_i is less reliable. Clearly, for all i, $0.5 < w_i \leq 1$.

Our scheme stores the final template T and the weight vector W for later use at verification time. Figure 2 illustrates calculation of T and W from a set of base templates.

At verification time, we obtain a fresh iris scan and generate an iris template T' from the scan using, once again, the method described in Section 2.1. We then retrieve T and W and compare T and T' according to the weighted normalized Hamming distance

$$HD_w(T, T', W) = \frac{1}{\sum_{i=1}^{n} w_i} \sum_{i=1}^{n} w_i(t_i \oplus t_i'). \qquad (3)$$

Figure 3 illustrates how we compare templates using weighted majority voting.

Fig. 2. Final template and weight vector generation at enrollment time. $T_1, T_2, \cdots, T_5$ represent base templates, T is the final template and W is the generated weight vector. Here we show 12-bit vectors for illustration, but the full vectors contain 9600 bits.

HD = 3.6/10.2 = 0.353

Fig. 3. Calculation of weighted Hamming distance. T is the enrollment-time final template, T' is the verification-time iris template, W represents the weight vector, and HD is the normalized weighted Hamming distance.

To incorporate the corrupted bits information in our scheme, we do a majority vote for the individual masks and generate a resultant mask. Using masking information, the normalized Hamming distance becomes

$$HD(T, T', M, M', W) =$$
$$\frac{\sum_{i=1}^{n}((t_i \oplus t'_i) \wedge m_i \wedge m'_i) \times w_i}{\sum_{i=1}^{n}(m_i \wedge m'_i) \times w_i}$$

$$(4)$$

where T and T' are the templates to match, M and M' are the corresponding masks, and W represent the weight vector.

Since the iris templates to be compared initially may not be aligned due to head tilt, we perform template alignment along with matching. We rotate the verification-time template 16 times (8 times in the clockwise and 8 times in the counterclockwise direction) by $1.5°$, and each time compare it with the corresponding enrollment-time template using either equation 3 or equation 4. The comparison that results in the lowest normalized Hamming distance among these 17 comparisons (1 original + 8 clockwise rotations + 8 counterclockwise rotations) is taken as the final Hamming distance between the two compared templates.

4. EXPERIMENTAL EVALUATION

4.1. Iris Database and Algorithm

We used CASIA version 1 [6] for our experiments. It consists of 7 iris images captured from each of 108 subjects, for a total of 756 images. The images were taken in two sets one month apart. We ran Masek and Kovesi's segmentation algorithm [12] on each of the 756 CASIA images. The algorithm accurately located the pupil and iris in 83% of the images. We manually located the pupil and iris in the remaining images then performed the rest of the base template extraction procedure as described in Section 2.1.

We should point out that CASIA version 1 has been criticized as an iris image database because the images have been altered to eliminate specular reflections in the pupil area [15]. However, although this makes the iris segmentation problem easier, in this paper, we treat iris segmentation and template generation as a black box. This means each of the bit weighting algorithms we compare benefit equally from the pupil alteration, and the relative performance of the bit weighting algorithms are not affected.

4.2. Evaluation Criteria

The accuracy of a biometric identification or verification system is usually measured in terms of its false acceptance rate (FAR) and false rejection rate (FRR), both of which depend on a distance or similarity threshold. To summarize these measures, we report the equivalent error rate (ERR), the point at which the FAR and FRR are equal.

Daugman [13] proposes *decidability*, similar to the d-prime measure from signal detection theory, as a better criterion for evaluating biometric systems. The decidability d' is given by

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{(\sigma_1^2 + \sigma_2^2)/2}}$$

where μ_1 and μ_2 are the means and σ_1 and σ_2 are the standard deviations of the within-class and between-class Hamming distance distributions, respectively.

Wides [16] suggests Fisher's ratio for biometric system evaluation. Fisher's ratio is given by

$$FR = \frac{(\mu_1 - \mu_2)^2}{v_1 + v_2}$$

where μ_1 and μ_2 are the means and v_1 and v_2 are the variances of within class and between class distributions, respectively.

We report all three criteria in our experiments.

4.3. Verification Results

To evaluate our weighted majority voting scheme, we performed two experiments, one without corrupted bit masking and one with corrupted bit masking. In both cases, we compared standard iris recognition (IR), reliable bit selection (IR-RB), majority voting (IR-MV), and weighted majority voting (IR-WMV) on CASIA. We computed Fisher's ratio, decidability, and the ERR for each experimental condition.

For IR-RB, IR-MV and IR-WMV, we used the first 5 CASIA images from each subject for training and used the remaining 2 images of each subject for testing. For IR, we used first image of each subject for training and used the remaining 6 images of each subject for testing.

For IR-RB, the final template has varying number of reliable bits for different subjects. In practice, the final template's size must be fixed to be no greater than the shortest length over all subjects, or some subjects would have to be discarded from the test. In our experiments, the shortest IR-RB template was 1361 bits, so we used a final template size of 1350 bits to evaluate the IR-RB scheme.

Table 1 summarizes the results of our experiments without masking. All three methods improve performance over standard iris recognition, but the proposed weighted majority voting scheme outperforms both reliable bit selection and majority voting. Figure 4 shows ROC curves for the four schemes. The figure shows that IR-WMV offers substantial improvement over IR and IR-RB, and in the critical region of very low false accept rates, our scheme is also superior to IR-MV.

	IR	IR-RB	IR-MV	IR-WMV
Fisher's Ratio	5.98	9.56	13.02	14.45
Decidability	3.46	4.37	5.1	5.38
EER (%)	3.73	3.24	1.45	1.39

Table 1. Comparison of iris recognition performance enhancement techniques without corrupt bit masking. The proposed system (IR-WMV) performs best according to all three criteria.

Neither Davida et al. [9] nor Yang et al. [10] used information about masked (corrupted) bits in their work. We modified their schemes to use masking and re-ran the experiment. Modifying IR-MV was straightforward. We did a majority vote for the individual masks and generated a "canonical" mask. In IR-RB, we considered only those bits as reliable for which no corresponding bit in any of its 5 masks was corrupted. The minimum final template size was found to be 745 bits and we used a 700-bit final template for their scheme.

	IR	IR-RB	IR-MV	IR-WMV
Fisher's Ratio	11.58	15.3	24.96	27.18
Decidability	4.81	5.53	7.06	7.37
EER (%)	0.83	1.85	0.08	0.06

Table 2. Comparison of iris recognition performance enhancement techniques with corrupt bit masking. The proposed system (IR-WMV) performs best according to all three criteria.
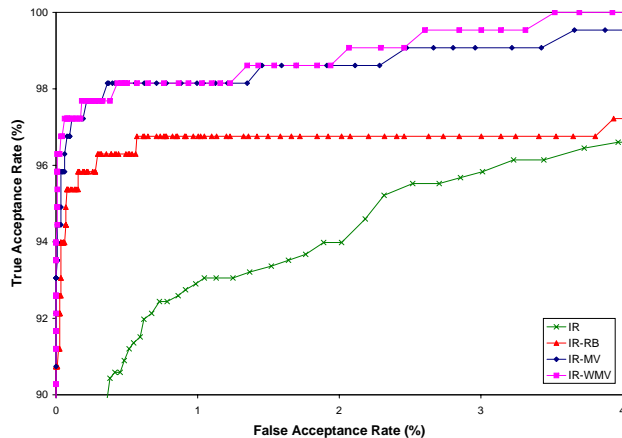
Fig. 4. ROC curves of iris recognition performance enhancement techniques without corrupt bit masking.

Table 2 summarizes the results of our experiments with the masked versions of these schemes. Both IR-MV and IR-WMV attain nearly perfect error rate. Due to space limitations, we omit the ROC curves for the masked versions of the schemes. The ROC curve for IR-WMV shows only a slight improvement over that for IR-MV.

5. DISCUSSION AND CONCLUSION

In this paper, we propose and evaluate a scheme for improving the accuracy of iris verification systems. As opposed to existing schemes, which either treat each bit equally or completely ignore unreliable bits, we use a distance measure that weights the bitwise comparisons according to the reliability of those bits at enrollment time. In two experiments on CASIA, one with corrupt bit masking and one without, we find that the method performs better than existing schemes using multiple enrollment-time scans to obtain more reliable templates. The method treats the template generation algorithm as a black box, so it can be used to improve the performance of any biometric verification system that employs bitwise comparison of binary templates.

The main limitation of the approach is that if imaging conditions are substantially different between enrollment time and verification time, the pattern of stable bits might change dramatically compared to the training set. This risk is inherent in any biometric authentication scheme, of course, but it does mean that the performance improvements will most likely decrease as the difference between enrollment time and verification time conditions increases.

In future work, we plan more extensive experimentation with larger, more difficult enrollment-time training sets. We expect that as the number of enrollment images increases, the advantage of weighted majority voting over other approaches will also increase.

6. REFERENCES

[1] 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.

[2] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, "A machine-vision system for iris recognition," *Machine Vision and Applications*, vol. 9, no. 1, pp. 1–8, 1996.

[3] W. W. Boles and B. Boashash, "A human identification technique using images of the iris and wavelet transform," *IEEE Trans. Signal Processing*, vol. 46, no. 4, pp. 1185–1188, Apr. 1998.

[4] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification based on iris patterns," in *International Conference on Pattern Recognition*, 2000, pp. Vol II: 801–804.

[5] Hugo Proena and Lus A. Alexandre, "UBIRIS: A noisy iris image database," in *Proceed. of ICIAP 2005 - Intern. Confer. on Image Analysis and Processing*, 2005, vol. 1, pp. 970–977.

[6] "CASIA Iris Image Database," Chinese Academy of Sciences - Institute of Automation (CASIA), 2004, `http://www. sinobiometrics.com`.

[7] M. Vatsa, Richa Singh, and P. Gupta, "Comparison of iris recognition algorithms," *Intelligent Sensing and Information Processing, 2004. Proceedings of International Conference on*, pp. 354–358, 2004.

[8] H. Proenca and L. A. Alexandre, "UBIRIS: A noisy iris image database," in *International Conference on Image Analysis and Processing*, 2005, pp. 970–977.

[9] George I. Davida, Yair Frankel, and Brian J. Matt, "On Enabling Secure Applications through Off-Line Biometric Identification," in *IEEE Symposium on Privacy and Security*, 1998.

[10] Shenglin Yang and I. Verbauwhede, "Secure IRIS Verification," in *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP*, 2007, pp. II–133–II–136.

[11] Libor Masek, "Recognition of human iris patterns for biometric identification," Tech. Rep., The School of Computer Science and Software Engineering, The University of Western Australia, 2003, `http://www.csse.uwa.edu.au/ ~pk/studentprojects/libor/index.html`.

[12] Libor Masek and Peter Kovesi, *MATLAB Source Code for a Biometric Identification System Based on Iris Patterns*, The School of Computer Science and Software Engineering, The University of Western Australia, 2003, `http://www.csse.uwa.edu.au/~pk/ studentprojects/libor/sourcecode.html`.

[13] John Daugman, "How Iris Recognition Works," in *IEEE Conference on ICIP*, 2002, pp. I–33– I–36.

[14] David J. Field, "Relations between the statistics of natural images and the response profiles of cortical cells," *Journal of the Optical Society of America A*, vol. 4, no. 12, pp. 2379–2394, 1987.

[15] P. J. Phillips, K. W. Bowyer, and P. J. Flynn, "Comments on the CASIA version 1.0 iris data set," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 10, pp. 1869–1870, Oct. 2007.

[16] R.P. Wildes, "Iris recognition: An emerging biometric technology," *PIEEE*, vol. 85, no. 9, pp. 1348–1363, September 1997.