2010 Fourth Pacific-Rim Symposium on Image and Video Technology

Bit Reliability-driven Template Matching in Iris Recognition

Christian Rathgeb and Andreas Uhl
Multimedia Signal Processing and Security Lab
University of Salzburg, Department of Computer Sciences
5020 Salzburg, Austria
Email: {crathgeb,uhl}@cosy.sbg.ac.at

***Abstract*—Of all the biometric applications available today, it is generally conceded that iris recognition is one of the most accurate. In the past several years a huge amount of iris recognition algorithms have been proposed. However, the vast majority of proposed algorithms restrict to extracting distinct features out of preprocessed iris textures to generate discriminative binary iris-codes, neglecting potential improvements in matching procedures.**

In this work we present a new technique for matching binary iris-codes. Information of authentication procedures is leveraged by maintaining so-called reliability masks for each user, which indicate local consistency of enrollment templates. Based on user-specific reliability masks a weighted matching procedure is performed in order to improve recognition performance. We apply the proposed matching procedure to different iris recognition algorithms and compare obtained recognition rates to other matching techniques. Experimental results confirm the worthiness of our approach.

***Keywords*-Biometrics; Iris Recognition; Biometric Template Matching; Bit Reliability;**

I. Introduction

Iris recognition is gaining popularity as a robust and reliable biometric technology. The iris's complex texture and its apparent stability hold tremendous promise for applying iris recognition in diverse application scenarios, such as border control, forensic investigations, as well as cryptosystems [1]. Several existing approaches to iris recognition (see [2]) achieve auspicious performance, reporting recognition rates above 99% and equal error rates of less than 1% on diverse data sets. The majority of proposed iris recognition algorithms build upon the work of Daugman [3], extracting binary iris-codes while simple metrices (e.g. fractional Hamming distance) are applied in the matching process. During enrollment image acquisition is performed and preprocessing is applied in order to extract iris textures. A representative iris-code is generated during feature extraction and stored as biometric template. At the time of authentication another image is acquired, preprocessed, and feature extraction is applied. The extracted iris-code is compared against the stored template in the matching procedure resulting in successful authentication or rejection.

Recent work [4] has shown that distinct parts of iris textures reveal more constant features (bits in the iris-code) than others. This is because some areas within iris textures are more likely to be occluded by eye lids or eye lashes. Additionally, parts of iris-codes which originate from analyzing the inner bands of iris textures are found to be more consistent than those parts which originate from analyzing the outer bands. Hence, masking out so-called "fragile" bits of iris-codes leads to a more accurate system.

The contribution of this paper is the proposal of new matching strategy of iris-codes, where we build upon the results observed in [4]. The proposed matching is referred to as *Bit Reliability-driven Template Matching*. In our matching procedure, information about previous matching processes is leveraged in order to detect the most reliable bits in iris-codes. For this purpose user-specific reliability masks are maintained which indicate the consistency of bit positions in stored iris-codes. Based on recorded information weighted matching is performed in order to improve recognition accuracy. Compared to existing approaches, which utilize weighted matching procedures (e.g. [5], [6]), our system does not require the acquisition of several enrollment samples. In contrast, initial user-specific weights are continuously refined after each successful authentication. Applying our approach to different iris recognition algorithms, we demonstrate that bit reliability-driven matching outperforms systems based on conventional matching procedures. Furthermore, the presented matching procedure is easily adopted to any existing iris recognition algorithm in which binary iris-codes are extracted.

The remainder of this work is organized as follows: first a brief overview of related work is given (Section II). Subsequently, the proposed system is described in detail (Section III). Experimental results are presented (Section IV) and a conclusion is given (Section V).

II. Related Work

Breakthrough work in iris recognition was proposed by Daugman [3]. Daugman's algorithm, in which iris images are mapped to binary iris-codes and similarity between codes is estimated by applying the Hamming Distance as metric, forms the basis of today's commercially used iris recognition systems. The majority of proposed iris recognition schemes (see [2]) build upon this concept where different algorithms are applied in the feature extraction stage.

978-0-7695-4285-0/10 $26.00 © 2010 IEEE
DOI 10.1109/PSIVT.2010.19

IEEE computer society

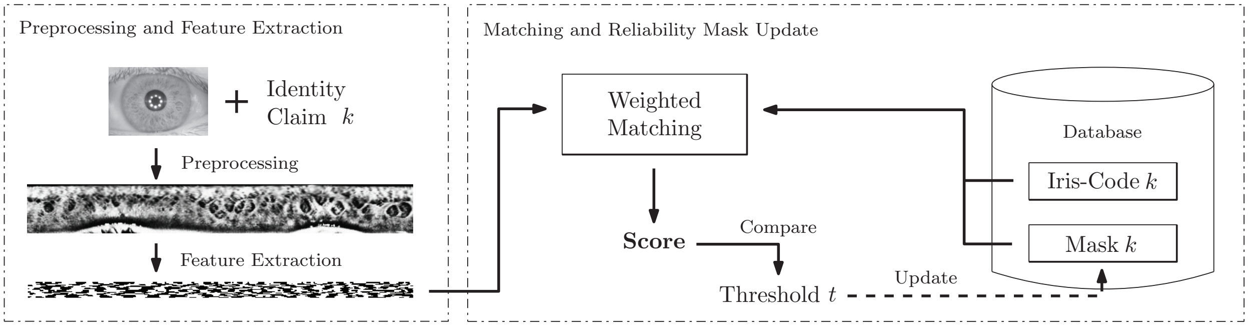

Figure 1. System Architecture: For each user registered with the system a reliability mask is stored, containing weights for each bit of stored iris-codes. At authentication weighted matching is performed and if the match score is below a predefined threshold the mask is updated.

Hollingsworth *et al.* [4] examined the consistency of bits in iris-codes resulting from different parts of the iris texture. The authors suggest to mask out so-called "fragile" bits for each user, where these bits are detected from several iris-code samples. In experimental results the authors achieve a marginal performance gain. Recently, we [7] have demonstrated that a context-based matching of binary iris-codes increases recognition rates as well. Within this approach iris-codes are arranged in a two-dimensional manner in order to detect clusters of matching as well as non-matching bits. Based on the idea that large connected matching parts of iris-codes indicate genuine samples and non-genuine samples tend to cause more randomized distortions according context-based match scores are extracted. To obtain representative user-specific iris template during enrollment Davida *et al.* [8] and Ziauddin and Dailey [6] analyze several iris-codes. While Davida *et al.* propose a majority decoding where the majority of bits is assigned to according bit positions, Ziauddin and Dailey suggest to assign weights to each bit position which are afterwards applied during matching. Obviously applying more than one enrollment sample yields better recognition performance [9], however, commercial applications usually require single sample enrollment.

III. System Architecture

The proposed system, which is illustrated in Figure 1, consists of several components where the main focus is put on the matching procedure. The entire scheme is described in more detail as follows:

A. Preprocessing and Feature Extraction

At preprocessing, the pupil and the iris of a given sample are detected by applying Canny edge detection and Hough circle detection. Having localized the pupil and iris circles, the area between them is transformed to a normalized rectangular texture of 512×64 pixel, according to the "rubbersheet" approach by Daugman. In a final step, lighting across the texture is normalized using blockwise brightness estimation.

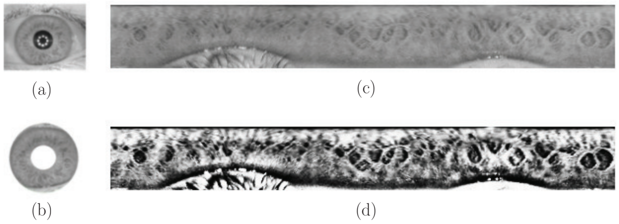

Figure 2. Preprocessing: (a) image acquisition (b) detection of the inner and outer iris boundaries (c) normalized iris texture (d) enhanced iris texture.

In the feature extraction stage, we employ custom implementations of two different algorithms extracting binary iris-codes. The first one was proposed by Ma *et al.* [10]. Within this approach the texture is divided into stripes to obtain 10 one-dimensional signals, each one averaged from the pixels of 5 adjacent rows (the upper 512×50 pixels are analyzed). A dyadic wavelet transform is then performed on each of the resulting 10 signals, and two fixed subbands are selected from each transform resulting in a total number of 20 subbands. In each subband all local minima and maxima above an adequate threshold are located, and a bitcode alternating between 0 and 1 at each extreme point is extracted. Using 512 bits per signal, the final code is then $512 \times 20 = 10240$ bit. The second feature extraction method follows an implementation by Masek[1] in which filters obtained from a Log-Gabor function are applied. Here, a row-wise convolution with a complex Log-Gabor filter is performed on the texture pixels. The phase angle of the resulting complex value for each pixel is discretized into 2 bits. Again, row-averaging is applied to obtain 10 signals of length 512, where 2 bits of phase information are used to generate a binary code, consisting of $512 \times 20 = 10240$ bit. The algorithm is somewhat similar to Daugman's use of Log-Gabor filters, but it works only on rows as opposed to the 2-dimensional filters used by Daugman. Preprocessing

[1] L. Masek: Recognition of Human Iris Patterns for Biometric Identification, Master's thesis, University of Western Australia, 2003

is shown in Figure 2. Examples of a preprocessed iris texture and the according iris-code, generated in the feature extraction step, are illustrated as part of Figure 1.

B. Matching and Reliability Mask Update

The proposed matching procedure represents the core part of the system. At the time of enrollment a binary iris-code I_K of length N is obtained from user K and stored as biometric template, $I_K \in \{0,1\}^N$. Additionally, a so-called "reliability mask" W_K of length N of weights, which should indicate the reliability of each bit of I_K is stored. Initially each value of W_K is set to 1. This means, initially all bits of I_K have the same consistency.

In generic iris recognition algorithms the similarity between two iris-codes I_K and I_L is determined by calculating the Hamming distance HD_{KL} of both bit streams such that,

$$HD_{KL} = \frac{\sum_{i=1}^{N} I_{Ki} \oplus I_{Li}}{N} \tag{1}$$

and if HD_{KL} is below a predefined threshold t, $HD_{KL} < t$, successful authentication is yielded. Additionally, bit-masking can be applied to mask out bits of iris-codes which originate from parts of the iris which are occluded by eye lids or eye lashes (bit-masks need to be extracted at each feature extraction).

In our matching process we calculate a weighted Hamming distance WHD_{KL} in order to estimate the similarity of two iris-codes I_K and I_L where the mask W_K of the claimed identity K is applied to weight the matching process,

$$WHD_{KL} = \frac{\sum_{i=1}^{N} (I_{Ki} \oplus I_{Li}) \cdot W_{Ki}}{\sum_{i=1}^{N} W_{Ki}} \tag{2}$$

At the first authentication $||W_K||$ is N since each bit of W_K is 1. Thus, WHD_{KL} is equivalent to HD_{KL}. But if successful authentication is achieved, that is, $WHD_{KL} < t$, for any extracted iris-code I_{Li}, the ith bit of the stored mask W_K of user K is updated such that,

$$W'_{Ki} = \begin{cases} W_{Ki} + (I_{Ki} \overline{\oplus} I_{Li}), & \text{if } WHD_{KL} < t \ , \\ W_{Ki}, & \text{otherwise.} \end{cases} \tag{3}$$

This means, upon each successful authentication weights of W_K are incremented at each position i where I_{Ki} is equal to I_{Li}, resulting in the updated mask W'_K. An example for the proposed matching procedure is illustrated in Figure 3. The predefined decision threshold t has to be set up according to the applied iris recognition algorithm (in generic iris recognition algorithms this threshold is settled around $HD = 0.4$). The threshold t remains unaltered for all users independent of the number of authentications. Since the weighted Hamming distance is calculated in relation to stored reliability masks inter-class distances are not expected to decrease. In contrast intra-class distances are expected to decrease due to the fact that unreliable bits are weighted less. We will confirm this claim in our experimental studies.

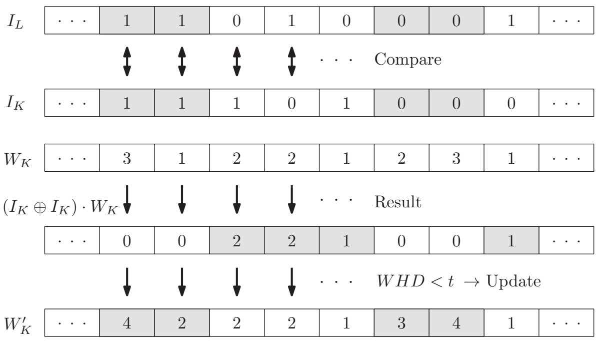
I_L | · · · | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | · · ·
· · · Compare
I_K | · · · | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | · · ·
W_K | · · · | 3 | 1 | 2 | 2 | 1 | 2 | 3 | 1 | · · ·
$(I_K \oplus I_K) \cdot W_K$
· · · Result
· · · | 0 | 0 | 2 | 2 | 1 | 0 | 0 | 1 | · · ·
· · · $WHD < t$ → Update
W'_K | · · · | 4 | 2 | 2 | 2 | 1 | 3 | 4 | 1 | · · ·

Figure 3. Proposed Matching: A weighted matching of iris-code bits is performed and according to matching bits the mask which contains user-specific weights is updated if the matching result is below a predefined threshold.

The proposed matching procedure exhibits several advantages: firstly, the proposed matching does not require the acquisition of several enrollment samples in order to detect reliable bits in iris-codes. Since the weighted matching process is still kept simple, running the system in identification mode is not expected to cause a drastic performance decrease. Furthermore, extracted weights are user-specific and after several successful authentications the mask of each user adopts to the iris-code extracted during enrollment. An example of this process is shown in Figure 4. As can be seen, after a small number of successful authentications the mask adopts to the stored iris-code. Less reliable parts of the iris-code, which result form parts of the iris texture which suffer from occlusions, tend to reveal low weights while others exhibit high weights. If a user-specific weighted matching is performed recognition rates improve as we will demonstrate

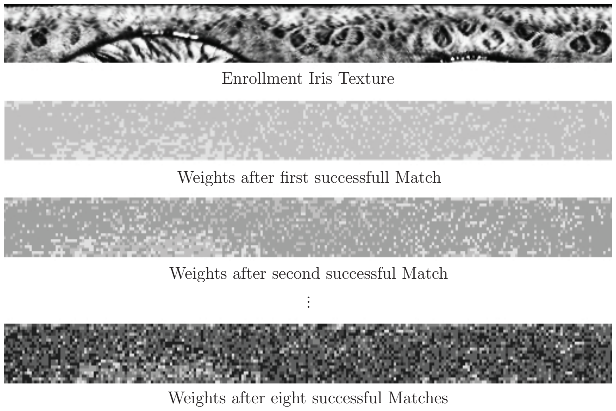
Enrollment Iris Texture
Weights after first successfull Match
Weights after second successful Match
⋮
Weights after eight successful Matches

Figure 4. Example of an reliability mask: Above: The iris texture used to enroll a user. Below: schematical impressions of the stored reliability mask after several successful authentications (dark regions indicate reliable parts of the stored iris-code)

in our experimental results.

Additionally masking bits can be easily integrated into the stored mask. We suggest to set the weights of stored masks zero if bits of a bit-mask indicate that iris-code bits result form parts of the iris texture where some kind of distortions were detected. Thus, the matching procedure does not need to be modified further and a bit-mask could be stored within the reliability mask. However, generic bit-masking does not represent an alternative to the proposed technique since conventional "two-dome" patterns do not cover all unreliable bits (see Figure 4) [4]. Furthermore, the proposed technique develops a multi-level distribution of reliability as opposed to binary bit-masking. Due to the fact that reliability masks are not binary (unlike bit-masks) additional memory will be necessary.

IV. Experimental Results

Experiments are performed using the CASIAv3-Interval[2] iris database, a widely used test set of iris images of over two hundred persons allowing a meaningful performance evaluation. The database comprises iris images of size 320×280 pixels where on average $\sim$ 7 images are available for each user. At preprocessing iris textures of 512×64 pixels are extracted as mentioned earlier. System performance is measured in terms of Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR) and Equal Error Rate (EER) which can be defined as follows: the genuine acceptance rate is ratio of truly matching samples, which are matched by the system and total numbers of tests. On the other hand the false acceptance rate is the ratio between the number of truly non-matching samples which are matched by the system and total number of tests. As score distributions overlap the EER value is defined at a certain point where 1-GAR = FAR. In our experiments the first image of each class is used to generate the enrollment sample. For inter-class matchings we only consider the first sample of each class, too. However, in order to provide a meaningful performance evaluation inter-class matchings are performed between each authentication sequence of genuine samples. Thus, we estimate the impact of reliability masks to inter-class matchings as well.

For the feature extraction algorithms of Ma and Masek the proposed matching is compared against other matching procedures (we do not consider matching procedures which require more than one enrollment sample). As mentioned earlier the easiest way of comparing two binary iris-code is to calculate the Hamming distance between them. The Hamming distance is a widely used metric since fast matching is essential in case large scale databases are applied. In order to confirm the worthiness of applying reliability mask we first investigate the performance of both algorithms after a certain number of authentication. The receiver operation curve (ROC) of the algorithm of Masek and Ma after several numbers of authentications are plotted in Figure 5 and 6, respectively (note that the number of intra-class matches increases). As can be seen, for both algorithms ROC curves originating from authentications where several genuine authentications have been performed before lie clearly below those where no or only a few genuine authentications have been performed. Additionally, we observe that convergence is achieved relatively fast. This means updating reliability masks may be stopped at a certain bit depth, reducing memory consumption (e.g. 3 or 4 bits per position).

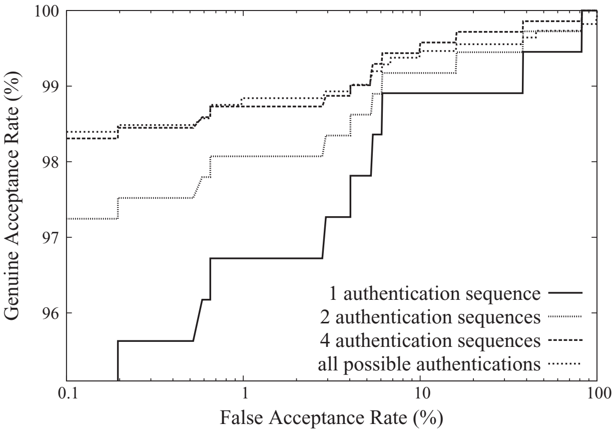

Figure 5. Receiver Operating Curve for the algorithm of Masek after a certain number of authentications.

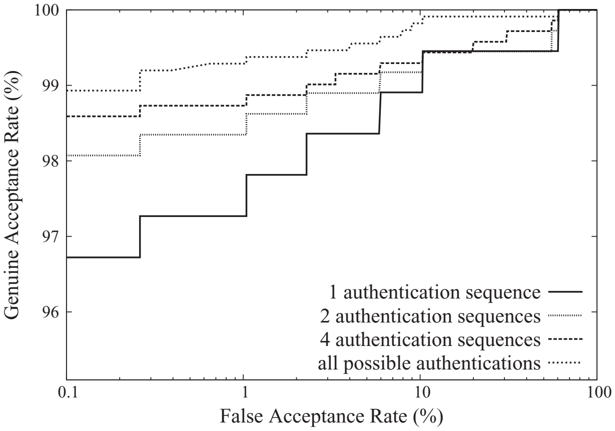

Figure 6. Receiver Operating Curve for the algorithm of Ma after a certain number of authentications.

Additionally, we compare the presented matching process to our recently proposed context-based template matching techniquel [7]. In this approach clusters of matching as well as non-matching bits are detected in order to obtain match scores. Intuitively, large connected matching parts of matching bits indicate genuine samples. Although some parts of genuine iris-codes may mismatch as well, these mismatching parts mostly occur due to the presence of eyelids

[2] The Center of Biometrics and Security Research, CASIA Iris Image Database, http://www.sinobiometrics.com

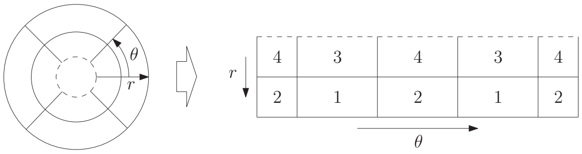

Figure 7. Global Weights: bits in iris-codes originating form the inner bands of iris textures reveal higher consistency than those of outer bands. Additionally, the top and bottom of the iris ring are often occluded by eyelashes or eyelids.

or eye-lashes, causing local distortions. On the other hand, large connected non-matching areas as well as rather small matching areas of iris-codes indicate non-genuine samples tending to cause more randomized distortions. Due to the complexity of the matching algorithm it is suggested to apply it in verification mode only. Furthermore, a matching procedure based on global weights is investigated. Based on the observations in [4] we assigned weights to iris-code bits depending on which part of the iris textures these originate from. Bits of iris-codes which originate from the inner bands of iris textures are found to be more consistent than those parts which originate from outer bands. Additionally, the top and bottom of the iris ring are often occluded by eyelashes or eyelids (315^o to 45^o and 135^o to 225^o). Hence, weights are assigned according to Figure 7 (high weights indicate high consistency). Weighted matching is performed as described in the proposed matching procedure. For matching to work well, for each matching procedure we compensate for eye tilt by shifting the bit-masks during matching by four pixels in each direction the best resulting match is compared against t. We did not employ any masking bits during performance evaluations.

For the feature extraction algorithm of Masek the receiver operation curves for applying the Hamming distance, context-based matching, global weights and the proposed bit reliability-driven matching are plotted in Figure 8. The according equal error rates (EER) are summarized in Table I. Applying the Hamming distance as metric an EER of 2.477% is obtained.

Algorithm	Matching	EER (%)
Masek	HD	2.477
	CB	2.039
	GW	1.699
	RD	1.254
Ma	HD	1.852
	CB	1.249
	GW	1.069
	RD	0.705

Table I
EQUAL ERROR RATES FOR THE ALGORITHM OF MASEK AND MA *et al.* FOR DIFFERENT SIMILARITY METRICES: HAMMING DISTANCE (HD), CONTEXT-BASED MATCHING (CB), MATCHING BASED ON GLOBAL WEIGHTS (GW) AND BIT RELIABILITY-DRIVEN MATCHING (RD).

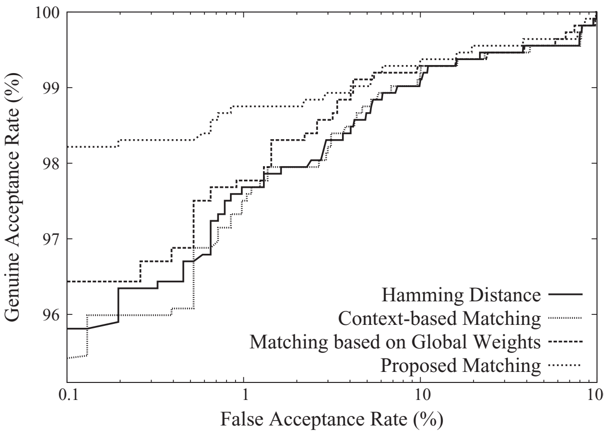

Figure 8. Receiver Operating Curve for the algorithm of Masek for different similarity metrices.

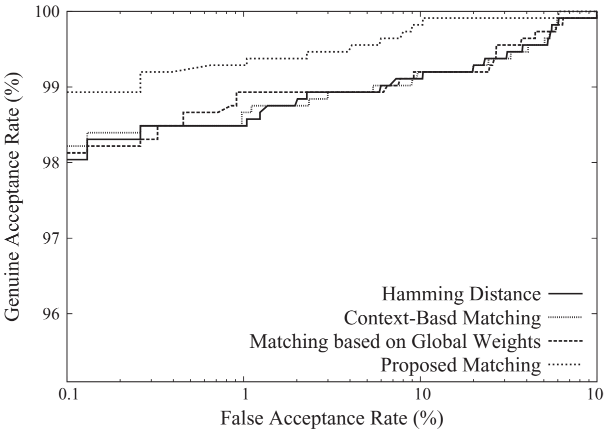

Figure 9. Receiver Operating Curve for the algorithm of Ma for different similarity metrices.

If context-based matching or matching based on global weights is performed performance is increased resulting in EERs of 2.039% and 1.699%, respectively. Best experimental results were achieved for the proposed matching, resulting in an EER of 1.254%. The same observation holds for the algorithm of Ma *et al.* as can be seen in Figure 9. For applying the Hamming distance in the algorithm of Ma *et al.* an EER of 1.852% is obtained. Again performance is increased if context-based matching and matching based on global weights is performed resulting in EERs of 1.249% and 1.069%. For applying the proposed matching an EER of 0.705% is achieved.

With respect to the complexity, bit reliability-driven matching reveals the same performance as any weighted matching procedure, since updating user-specific reliability masks is performed after successful authentication (in case of identification only masks of rank-1 candidates are updated). However, as experiments demonstrate, applying user-specific weights the performance is increased even more. For applying bit reliability-driven template matching to the algorithm of Masek and Ma *et al.* the EER is decreased from 2.477% to 1.254% and from 1.852% to 0.705%, respectively. These are promising results which confirm the soundness of the proposed matching strategy.

V. Summary and Conclusion

In this work we presented an efficient approach to comparing iris-codes which we refer to as bit reliability-driven matching. By leveraging information of successful authentications, weights, which indicate consistency of distinct bits, are assigned to each user stored in a separate mask. The proposed matching algorithm does not require the acquisition of several enrollment samples to generate user-specific reliability mask, rather these masks are refined after each successful authentication. Thereby, reliability masks are continuously adopted to stored enrollment samples. Experimental results show that the presented technique outperforms existing approaches to template matching. We applied our bit reliability-driven matching to different implementations of iris recognition algorithms where recognition rates are increased noticeably.

Acknowledgment

This work has been supported by the Austrian Science Fund, project no. L554-N15.

References

[1] A. Ross, “Iris recognition: The path forward,” *Computer*, vol. 43, pp. 30–35, 2010.

[2] K. Bowyer, K. Hollingsworth, and P. Flinn, “Image understanding for iris biometrics: A survey,” *Computer Vision and Image Understanding*, vol. 110, no. 2, pp. 281 – 307, 2008.

[3] J. Daugman, “How Iris Recognition Works,” *IEEE Trans. CSVT*, vol. 14, no. 1, pp. 21–30, 2004.

[4] K. P. Hollingsworth, K. W. Bowyer, and P. J. Flynn, “The best bits in an iris code,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 964–973, 2009.

[5] S. Yang and I. Verbauwhede, “Secure Iris Verification,” in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP 2007)*, vol. 2, 2007, pp. II–133–II–136.

[6] S. Ziauddin and M. Dailey, “Iris recognition performance enhancement using weighted majority voting,” in *Proceedings of theh 15th International Conference on Image Processing, ICIP ’08*, 2008, pp. 277–280.

[7] C. Rathgeb and A. Uhl, “Context-based Template Matching in Iris Recognition,” in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP 2010)*, 2010, pp. 842–845.

[8] G. Davida, Y. Frankel, and B. Matt, “On enabling secure applications through off-line biometric identification,” *Proc. of IEEE, Symp. on Security and Privacy*, pp. 148–157, 1998.

[9] Y. Du, “Using 2D log-Gabor spatial filters for iris recognition,” *SPIE 6202: Biometric Technology for Human Identification III*, pp. 62 020:F1–F8, 2006.

[10] L. Ma, T. Tan, Y. Wang, and D. Zhang, “Efficient Iris Recogntion by Characterizing Key Local Variations,” *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 739–750, 2004.