IRIS BIOMETRICS FOR SECURE REMOTE ACCESS

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk
Warsaw University of Technology, Institute of Control and Computation Engineering, Poland
Research and Academic Computer Network NASK, Biometrics Laboratory, Poland

Abstract: We propose a new iris texture coding technique with optimal feature extraction, and design a secure remote (internet) access system using the proposed biometrics. The proposed iris coding method is based on Zak-Gabor coefficients sequence, and additionally uses an optimal selection of a subset of iris features. The secure access involves a communication scenario that employs a usual client-server network model, thus incorporating standard security mechanisms with biometric enhancements. The proposed access scenario enables to include the aliveness detection capability and the biometric replay attack prevention.

Keywords: Biometrics / iris / optimal features / remote access security

1. INTRODUCTION

The ideal biometrics may be envisioned as a physical or behavioral characterization of a person and a method of its symbolic description, fused in a system that is resistant to counterfeits, produces no authentication errors, is immune to aging and diseases, brings no social, religious, ethical, and other objections, and finally, is comfortable in use.

Biometrics research is still looking for this ideal. A wide variety of biometric modalities have been investigated and applied to various access control scenarios, including fingerprints, iris, face, voice recognition, hand geometry, handwritten signatures, etc. At present, fingerprint analysis is quite widely used, yet iris-based authentication is another important candidate for being a source of highly distinctive attributes characterizing identity with high reliability. It is fast, highly reliable and completely non-invasive, is stable throughout the human life and independent of genetic features [A2], and raises little social objections. The iris-based authentication seems to be close to ideal and is likely to prevail over its competitors.

The iris texture complexity is very high and may need non-trivial feature extraction and coding algorithms and large computation times. The iris authentication methodology has been pioneered by John Daugman, and

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

the commercial solutions are based on his algorithms. There still may be a need for new solutions, aiming into fast robust feature extracting.

In the paper we propose a new method of iris texture coding and feature extraction, and its application to internet security. We shortly introduce the iris coding method based on Zak-Gabor coefficients sequence, the routines for optimal iris features selection, and we show how these ideas may be implemented into a secure remote access system. A prototype of remote such authentication device was built and tested with the use of an iris database.

2. EYE IMAGING

2.1. Imaging Hardware

Before any type of processing, the iris images must first be captured. In this order, we use Iris Imaging Device which is a part of NASK Iris Recognition System prototype (Figure 1). The system consists of an eye imaging analogue camera with 570 TV lines resolution equipped with motorized lens, a framegrabber board for image acquisition, near-infrared illuminators placed on both sides of the lens, and a workstation controlling the hardware and processing acquired images. The imaging system interacts with a volunteer during the imaging process and helps him/her to position his/her head correctly behind the camera lens. Once the hardware encounters the eye existence in a proper distance and position, it starts to acquire a sequence of frames with varying focal length, thus compensating small depth-of-field that is common in imaging small targets as the human iris. The acquisition process takes approximately one second, and the whole iris image capturing including eye positioning approximates to 5 seconds. The iris images are compliant with the rectilinear iris image requirements as required by ISO/IEC 19794-6 Final Committee Draft [D3].

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

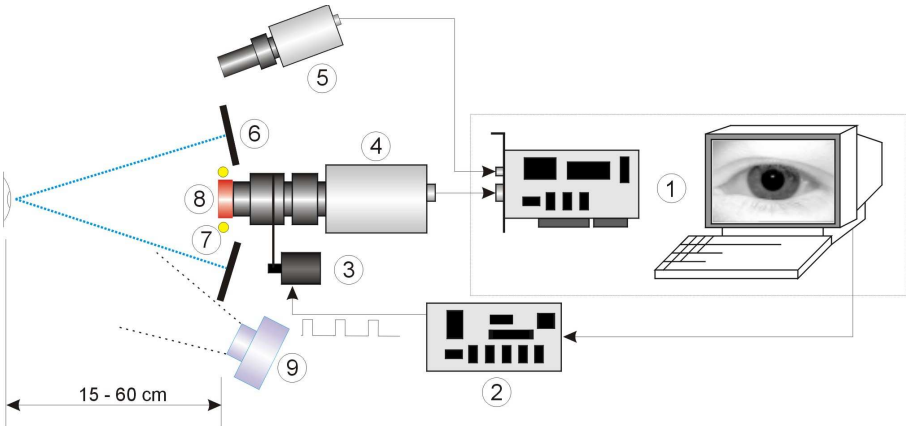

Figure 1. Iris image acquisition prototype as developed in NASK. The prototype consists of the workstation controlling the hardware and processing iris images (1), iris imaging camera (4), eye surroundings imaging camera (5), lens motor (2,3), positioning mirrors (6) and positioning LEDs (7), infrared filter (8), infrared illuminators (9).

The above hardware was used to create at NASK a multimodal biometric database BioBase, which at present contains images of iris, face, hand shape, and handwritten signatures, of couple of hundred volunteers. BioBase will be employed here to test the proposed approaches.

2.2 Iris Body and Occlusions Localization

Camera raw image contains the iris and its surroundings. Thus, the iris localization methods must be applied to extract the valuable iris texture information available within the image. Localization of both inner (i.e., between the pupil and the iris) and outer (i.e., between the iris and the sclera) iris boundaries makes use of local image gradient estimation. Consequently, we approximate the shape of inner and outer boundaries by two non-concentric circles. Figure 2 presents the camera raw image with iris both circular boundaries localized.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

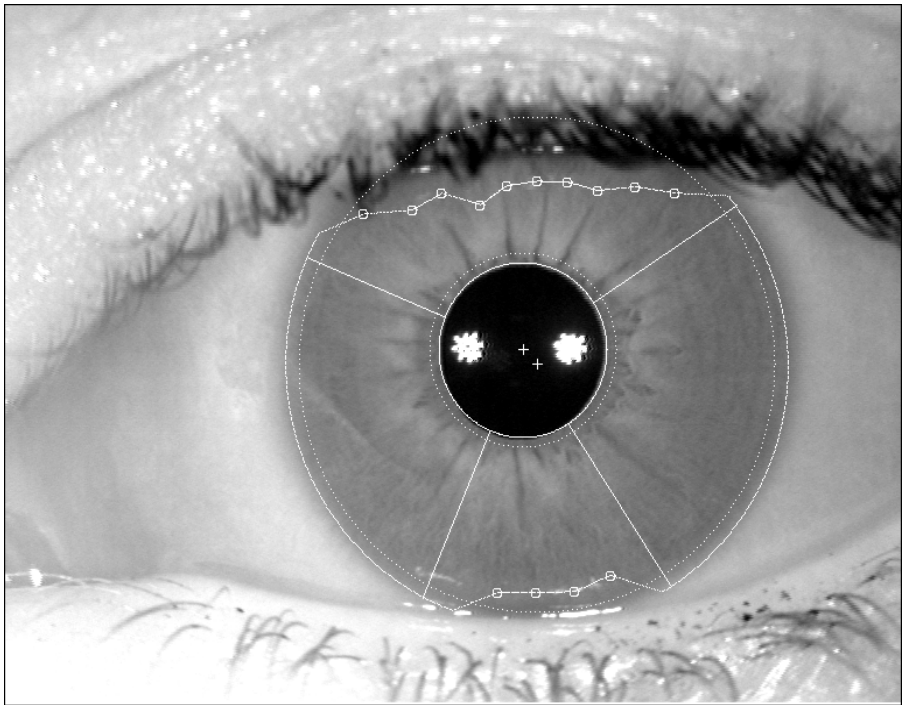

Figure 2. Pre-processing of the raw iris image: detection of occlusions (circled lines) and iris sectors free of occlusions (white lines).

The extracted iris body is almost always occluded by eyelids, or interfered with specular reflections as the effect of infrared illumination (cf. Fig. 2). Thus, we apply the method of localizing the iris texture occlusions through detecting of inconsistent iris structure points. First, iris texture irregularity in radial direction is investigated at several angular positions. Afterward, estimating the maximal inconsistency for a particular iris image, we compare this result with inconsistency for radial directions determined for a number of angular sections. Consequently, we end up with a map of occlusion points for a number of angular sections.

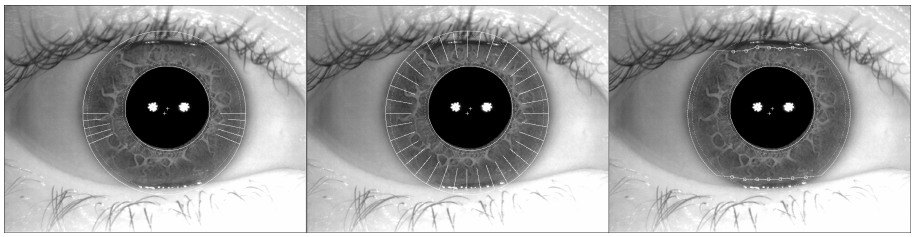

Figure 3. (left) Image regularity determination in typically free of occlusions iris sections, (middle) irregularity check in all angular sections, (right) iris occlusions detected.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

2.3 Iris Body Representation

Zak-Gabor algorithm makes use of a rectangular iris image representation. The inner and the outer iris boundaries are approximately circular, yet are not concentric. It is thus useful to transform the iris image to a rectangular representation by a resampling. Two iris sections free from eyelids and reflections, each of the angular width of 90^o, are used in further image analysis, see Figure 4. Denote by P the iris sector angular width and by H its height.

The experiments (see also [A2]) revealed much higher correlation of the iris body in the radial direction as compared to the angular direction. Thus, instead of analyzing 2D images, we represent both iris sectors (in rectangular coordinates) as a collection of R iris stripes (R/2 stripes for each iris sector). Angular fluctuations of the iris structure are represented by the stripe variability, while radial fluctuations are averaged over a certain horizon.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

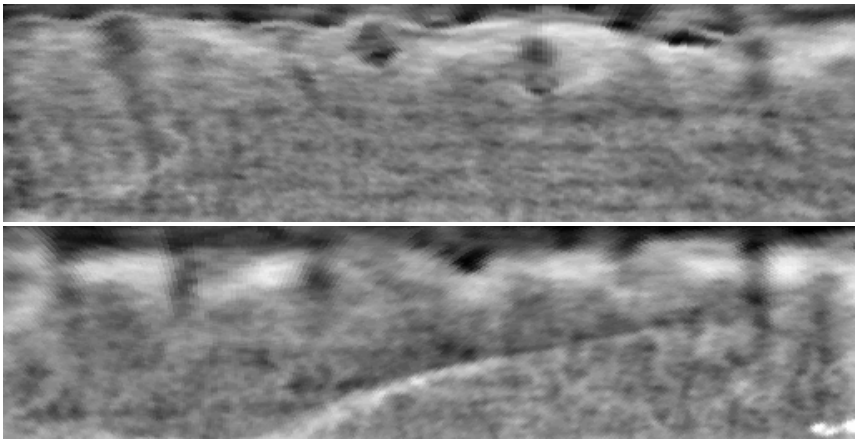

Figure 4. Left and right iris angular sectors in rectangular coordinates, as determined for iris image depicted in Fig. 2

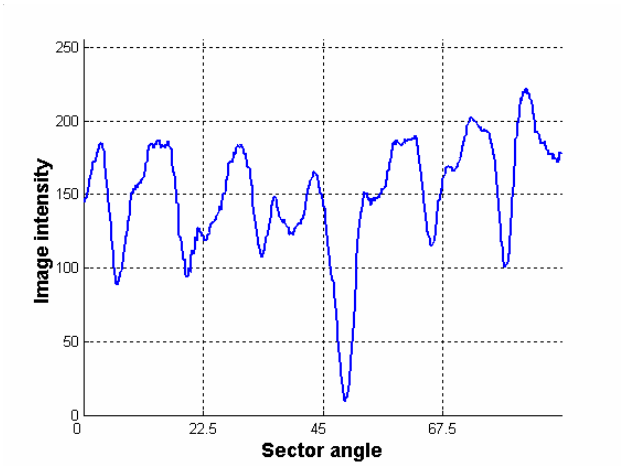

Figure 5. Intensity fluctuations in a single stripe, as determined for angular sector shown in Fig. 4.

Presented iris acquisition system is equipped with a coding method (see Sec. 3) to make it possible to observe and enhance the iris recognition process. Tables 1 and 2 present the average processing times in the current version of NASK Iris Recognition Device.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

Table 1. Raw iris image acquisition times when using NASK Iris Recognition Device

Task	**Average processing time [s]**
Skilled volunteer head and eye positioning	approx. 2.5
Frames collection acquisition	approx. 1.0
Best quality frame selection	approx. 1.5
Total	**approx. 5.0**

Table 2. Raw iris image processing times when using NASK Iris Recognition Device

Task	**Average processing time [s]**
Iris boundaries localization and occlusions detection	2.819
Representation of iris image as a sequence of stripes	0.586
Zak-Gabor coefficients calculation and transformation into a features vector	0.06
Matching	< 0.01
Total	**3.47**

3. IRIS CODING

3.1. Gabor Expansion

It is often convenient to characterize a discrete-time signal in the frequency domain, or in a joint time-frequency domain, thus describing a stationary frequency distribution of energy. The common and well known mathematical tool for frequency analysis is the Fourier transform, typically in the form of Fast Fourier Transform. Sometimes, for non-stationary signals, it is fruitful to characterize the frequency locally, and find the

distribution of signal energy in local – possibly overlapping – time segments. Typical examples of applications of this approach include sound analysis, like music applications, human voice recognition and biometric speaker verification. Pattern analysis is a second important application domain of time-frequency techniques, where the purpose of analysis is to differentiate (or recognize, segment, identify, etc.) local areas of incoming data by a use of local filters. In many cases it is fruitful to characterize these filters by position and scale instead of time and frequency.

Iris texture analysis may be qualified as a 2D pattern analysis task, yet it is often simplified to a set of 1-D tasks. The analysis aims at describing local features of iris, so that to construct a compact feature vector. Time-frequency or scale-frequency analysis seems to be a natural candidate to solve this problem. One of possible approaches is Gabor's signal expansion [C1], where a continuous-time signal is presented in a form of a set of properly shifted and modulated elementary (arbitrarily-shaped) signals. Typically, the elementary signals are Gaussian-shaped, since they result in best time-frequency resolution. In other words, Gaussian-shaped elementary signals (shifted and modulated) occupy the smallest possible area in the time-frequency domain. Gaussian-shaped elementary signals are yet not orthogonal, so Gabor's expansion coefficients cannot be determined in a simple way. Suggested algorithms include making the window function bi-orthonormal to the Gaussian-shaped elementary function [C3], the matrix-based algorithm [C6], and Zak transform [C3,C6]. Both matrix-based algorithm and the Zak-Gabor transform result in direct Gabor's coefficients calculation. Determination of Gabor's expansion coefficients through the Zak transform, developed by Martin J. Bastiaans [C3], is often called Zak-Gabor transform and is the fastest method for this purpose. We shortly describe this approach.

Denote by *g* a one-dimensional Gaussian function characterized by a scale parameter *D*, sampled at points 0 ... *P*-1, namely

$$g[p] = 2^{\frac{1}{4}} e^{-\pi([p+\frac{1}{2}]/D)^2}, \quad p = 0 \ldots P-1 \tag{1}$$

We describe the Zak-Gabor transform for a single stripe and a chosen fixed scale parameter *D*. Let *M* be a number of translations of *g*, and *K* be the number of frequency shifts where we always take *M*=*P*/*K*. The Gabor elementary functions (GEF), are defined as shifted and modulated versions of *g*, namely

$$g_{mk}[p] = g[p - mK] e^{ikp2\pi/K}, \quad p = 0 \ldots P-1 \tag{2}$$

where m and k denote position and frequency shifts, respectively (m=0,1,…,M-1, k=0,1,…,K-1), and g is wrapped around P point domain. Denote by f the intensity function defined on a stripe. The finite discrete Gabor transform of f is defined as a set of complex coefficients a_{mk} that satisfy the Gabor signal expansion relationship, namely

$$f[p] = \sum_{m=0}^{M-1} \sum_{k=0}^{K-1} a_{mk} g_{mk}[p], \quad p = 0 \ldots P-1 \tag{3}$$

Following Bastiaans [C3], we set K=D in further analysis so that the scale D parameter together with the stripe size P determine both M and K.

3.2. Zak transform

The discrete finite Zak transform $Zf[\rho,\phi;K,M]$ of a signal f sampled equidistantly at P points is defined as the one-dimensional discrete Fourier transform of the sequence $f[\rho+nK]$, n=0,...,M-1, namely [C3]

$$\mathcal{Z} f[\rho, \phi; K, M] = \sum_{n=0}^{M-1} f[\rho + nK] e^{-in\phi 2\pi/M} \tag{4}$$

where M=P/K. The discrete Zak transform is periodic both in frequency ϕ (with the period $2\pi/M$) and in location ρ (with the period K), we choose the values of ρ and ϕ within the fundamental Zak interval, namely ρ=0,1,…,K-1 and ϕ=0,1,…,M-1.

Similarly to the Fourier transformation, one may reconstruct the original function f from its Zak transform by way of the inverse discrete Zak transform, using the formula

$$f[\rho + nK] = \frac{1}{M} \sum_{n=0}^{M-1} \mathcal{Z} f[\rho, \phi; K, M] e^{in\phi 2\pi/M} \tag{5}$$

simultaneously restricting the domain of the results to the fundamental Zak interval.

3.3. Application of Zak transform in Gabor transformation

Gabor's expansion coefficients can be recovered from the product form (8). In fact, application of the discrete Zak transform (5) to both sides of (3) yields

$$\mathcal{Z}f[\rho,\phi;K,M]=\sum_{n}^{M-1}\left[\sum_{m}^{M-1}\sum_{k}^{K-1}a_{mk}g[\rho+nK-mK]e^{ik\rho 2\pi/K}\right]e^{-in\phi 2\pi/M} \tag{6}$$

Rearranging the factors in (6) to

$$\begin{aligned}\mathcal{Z}f[\rho,\phi;K,M]=\\ \sum_{n=0}^{M-1}\left[\sum_{m=0}^{M-1}\sum_{k=0}^{K-1}a_{mk}g[\rho+nK-mK]e^{ik\rho 2\pi/K}e^{-im\phi 2\pi/M}e^{im\phi 2\pi/M}\right]e^{-in\phi 2\pi/M}=\\ \sum_{m=0}^{M-1}\sum_{k=0}^{K-1}a_{mk}e^{-i2\pi(m\phi/M-k\rho/K)}\left[\sum_{n=0}^{M-1}g[\rho+(n-m)K]e^{-i2\pi(n-m)\phi/M}\right]\end{aligned} \tag{7}$$

results in

$$\mathcal{Z}f[\rho,\phi;K,M]=\mathcal{F}a[\rho,\phi;K,M]\,\mathcal{Z}g[\rho,\phi;K,M] \tag{8}$$

where $Fa[\rho,\phi;K,M]$ denotes the discrete 2D Fourier transform of the signal a, and $Zg[\rho,\phi;K,M]$ is the discrete Zak transform of the Gaussian window used in the Gabor transformation. It shows that Gabor's expansion coefficients can be easily recovered from the product form (8). Once we choose K and M to be a power of 2 (hence the signal length P is a power of 2), calculation of both $Zf[\rho,\phi;K,M]$ and $Zg[\rho,\phi;K,M]$ and inverting 2D Fourier series rely on the Fast Fourier Transform, yielding computation times proportional to those in the FFT.

3.4. Determination of iris features based on Zak-Gabor coefficients

Gabor expansion coefficients (Sec. 3.1) were defined for a single scale parameter D and all strips r=0,…,R-1. To determine the iris features we determine Gabor expansion coefficients for chosen scales $D \in \boldsymbol{D}$, where $\boldsymbol{D}$ is the set of scales, ending up with a family of coefficients indexed by the quadruple: within-stripe position, frequency index, stripe index and scale

(*m*,*k*,*r*,*D*). Identically as in Daugman's representation calculations, we define the features b_n as the signs of the real and imaginary parts of Zak-Gabor coefficients as features, namely

$$\mathrm{sgn}(\Re(a_{mk;rD}), \quad \mathrm{sgn}(\Im(a_{mk;rD})) \tag{9}$$

where m=0….,M-1, k=0…K-1, r=0,…,R-1, $D \in \boldsymbol{D}$. The total possible number of Zak-Gabor coefficients $PR\,\#\boldsymbol{D}$, where # denotes the number of elements in a set, thus leads to the *maximal feature vector b* of N=2$PR\,\#\boldsymbol{D}$ elements. We later select a subset of features to be included in an *optimal feature vector* b^*. We will keep the order of features identical for all images. Hence, the matching requires only XOR operation between two feature vectors, and the Hamming distance is used as the matching score between two irises.

3.5. Choice of optimal features

The number of features in the maximal feature vector, of order of hundreds of thousands, is too big to be useful in practice, due to such issues like data transmission through the net, data storage in databases, templates comparison made in smart card processors or biometric standalone devices, etc. To reduce the number of features, we will look for a feature vector that leads to minimum sample equal error rate determined on available iris images database.

3.5.1. Optimization of features

To find features that carry most information, we will first analyze the sample variances of features. Since the set of all data can be divided into classes, each corresponding to a different eye, we can define average within-class sample variance $s_n^{(w)}$, and between-class sample variances by $s_n^{(b)}$, for each feature b_n given by (9). The features can now be selected in such a way that the between class separation is maximized and the within class separation is minimized, with the separations measured by the respective sample variances. Intuitively, a feature is useful if at least $s_{\min}^{(b)} < s_n^{(b)} < s_n^{(w)}$ where $s_{\min}^{(b)}$ is a between-class variance low threshold. Typically, the number of bits that meet this requirement is still too high. Moreover, the features are often highly correlated, thus carrying similar information. It is thus useful to introduce stronger selection mechanisms that select features b_n of low within-class sample variance and high between-class sample

variance. This prioritizing my be done by sorting the features by a decreasing values of the variance quotient q_n, defined as

$$q_n = \frac{s_n^{(b)}}{s_n^{(w)}} \tag{10}$$

In order to minimize the sample correlation while sorting the features, we select only those consecutive elements for which the sample correlation coefficients with all the elements already selected does not exceed an assumed correlation threshold. We denote the selected bits by b_n^*, n=0,…,N^*-1 where $N^* \leq N$. They are related to Zak-Gabor coefficients characterized by various quadruples (m,k,r,D), cf (9).

To study the relation between the number of features and the system quality, we may use one of standard measures that characterize the difference between two random variables. Assume that the scores c_b and c_w, related to comparisons between different and the identical eyes, are independent random variables. The *decidability* (or *detectability*) [A2] is defined as

$$d = \frac{|\overline{c}_b - \overline{c}_w|}{\sqrt{\frac{1}{2}(\overline{\overline{c}}_b + \overline{\overline{c}}_w)}} \tag{12}$$

where $\overline{c}_b$, $\overline{c}_w$ denote the sample means and $\overline{\overline{c}}_b$, $\overline{\overline{c}}_w$ denote sample variances of c_b and c_w, respectively. The value of d estimates the degree by which the distributions of c_b and c_w overlap (the higher d is, the lower is the overlap). The decidability changes with the number of features included in the feature vector (Fig. 6). We estimated d using the iris data in BioBase, and found out that with the number of features (sorted as described above) growing to more that 100 000, the decidability first grows to reach a maximum for 324 features, and then decreases. At the maximum, there is no overlap of c_b and c_w distributions, i.e., there are no false matches and no false non-match examples. This 324-bit vector is an intermediate iris feature vector employed in the second selection stage.

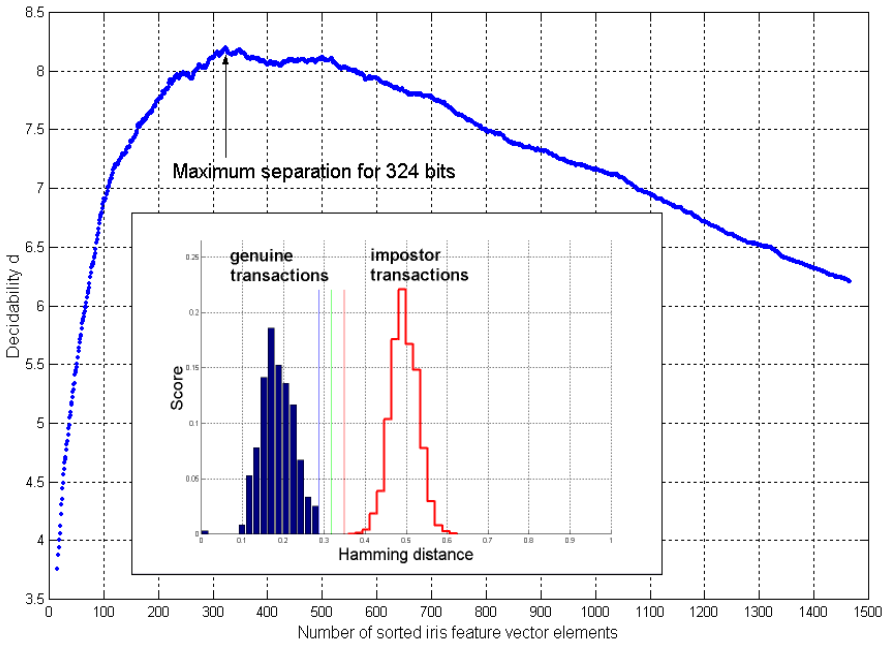

Figure 6. Decidability coefficient d vs. the number of sorted iris features. Best d was obtained for 324 bits. The corresponding genuine and impostor score distributions are presented in the inset.

3.5.2. Optimization of feature classes

The scales and frequencies of Zak-Gabor coefficients included into the code have a strong influence on the overall method's efficiency. Since D and k are dependent, they should be considered simultaneously. Their optimal selection is complicated, since we cannot a priori guess the most common frequencies that characterize all iris images, due to huge and unknown iris texture variability.

One may assume a uniform distribution of the information along the iris and aim into selecting "the best" frequency-scale pairs (k,D). This can be done by grouping in one class all coefficients of the same frequency-scale pair (k,D), and enlarging the feature vector by all features in a class. In other words, the problem is to find the best frequency-scale pairs.

Note that the number of features included in the feature vector b^* is not identical for all classes. The sorting rule for the classes of features mirrors the rule used for features: we sort the classes by the decreasing number of elements included into the feature vector. This enables to find the frequency-scale pairs for which the distributions of c_b and c_w are best separated. In other words, this procedure selects the features most sensitive to eye texture variability that characterize the individuals.

If there are no false matches and no false non-match errors for the tested database, we define the separation margin *s* as the difference between the worst (the lowest) between-class comparison score and the worst (the highest) within-class comparison score.

We calculated both *d* and *s* for various numbers of feature classes used in features calculations, and chose classes (scale-frequency pairs) characterized by the maximal *d*. This leads to the iris feature vector of 1152 bits (144 bytes) containing only four feature classes (Fig. 7). Simultaneously, for those four selected feature classes we achieved the maximal non-zero separation *s*.

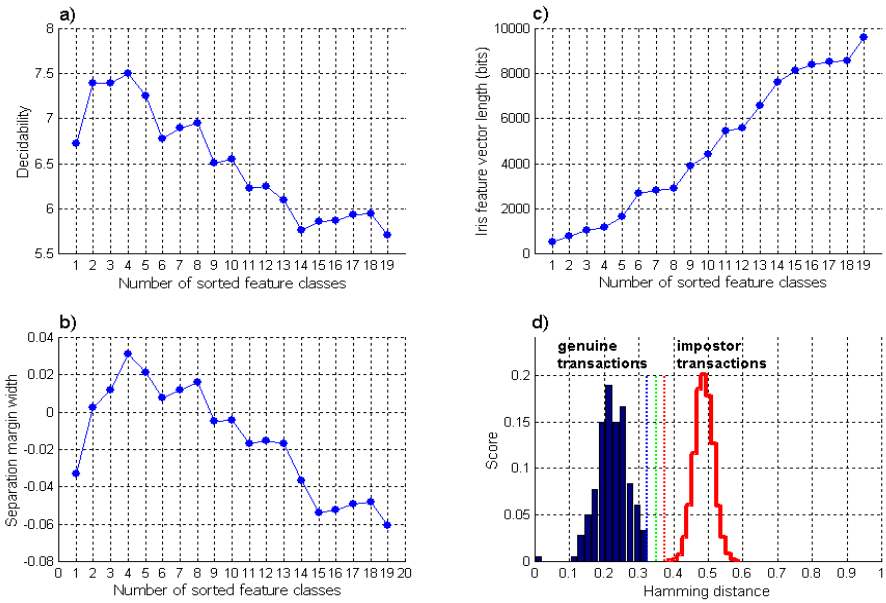

Figure 7. a) Decidability *d* vs. number of sorted frequency-scale pairs included in the feature vector, b) the separation margin *s*, c) the length of the iris feature vector, d) distribution of comparison scores for the same and different irises for the best final 144 byte iris feature vector.

We verified the above feature vector using the iris data for 180 individuals included in BioBase, with four images per volunteer available, three used for template creation and one employed in verification trials (Fig. 8). We obtained zero false matches and zero false non-matches.

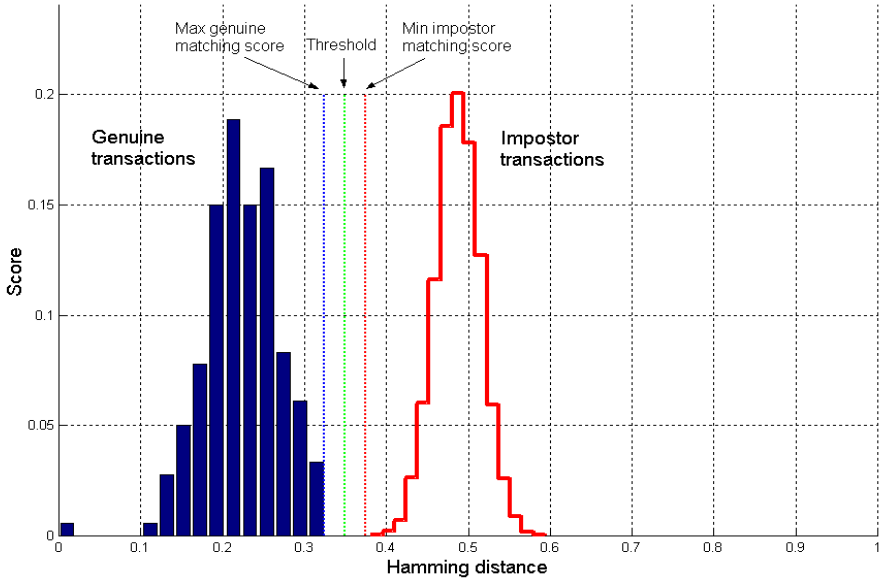

Figure 8. Comparison scores for iris data in NASK BioBase. 180 (*N*) genuine and 32220 (*N*(*N*-1)) comparisons impostor transactions were used. The average genuine transaction score 0.22, the average impostor transaction score 0.48, the minimal impostor transaction score 0.37, maximal genuine transaction score 0.32, Threshold = 0.35 results in no sample false match and no sample false non-match errors.

4. IRIS VERIFICATION FOR REMOTE ACCESS

4.1. Remote Access Scenario

Biometrics can be used in granting the remote access to the network. The scenario employs a common client-server network model, thus incorporating standard security mechanisms with biometric enhancements. The client terminal (see Fig. 9) is a biometric-based host, equipped with the capturing device and the processing unit that measures the biometric trait and calculates the features vector (biometric template). The client capabilities may be understood in a wider sense, thus enabling the client to be equipped with sensors related to more than one biometric modality. The proposed access scenario enables to include the aliveness detection capability and the biometric replay attack prevention. To insert the necessary elements into the communication flow, capture-dependent parameters will be retrieved by the client terminal prior to the biometric trait measurement.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

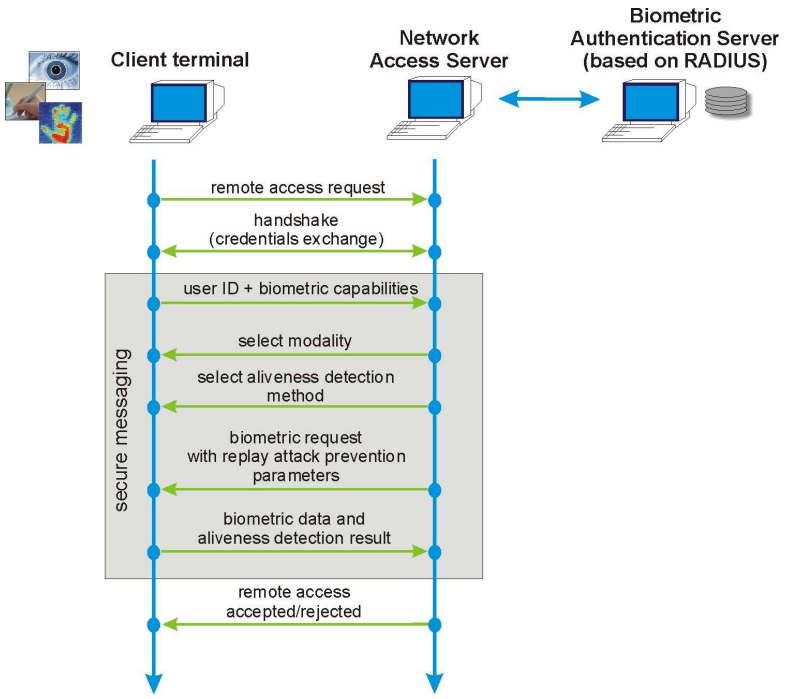

Figure 9. Biometric remote network access scenario. Single remote network access is depicted in a form of the EAP packets exchange between the biometric client and the biometric authentication server.

A flexible solution of biometric remote authentication can be based on biometric enhanced EAP protocol included in RADIUS server. RADIUS can incorporate a number of authentication protocols, e.g., PAP, SPAP, CHAP, MS-CHAP, EAP, depending on the distribution. The EAP protocol (*Extensible Authentication Protocol*) – among those available – can be extended for additional authentication methodology. Figure 9 presents the proposed EAP packets exchange in case of the biometric remote authentication, with aliveness detection and biometric replay attack prevention. Note that the client terminal may require some volunteer-dependent parameters prior to the capturing process (e.g., position and size of the iris sectors, left/right eye/hand/ear, the fingerprint index, the handwritten signature phrase, etc.). These additional parameters may be used for biometric replay attack prevention, since the server may require different parts of the biometric traits in each transaction. Additionally, the same mechanism of using additional parameters may be useful in dynamic biometrics implementations (e.g., phrase-dependent voice verification), when the challenge-response mechanism is necessary.

The above scenario is generic and may be applied to iris-based authentication. In particular, iris recognition with Zak-Gabor iris coding methodology can be applied here.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

The client workstation can be established on Windows 2000 system and configured to enable for VPN connection to the remote network. Windows 2003 Server can be used as Network Access Server (NAS) for this purpose. The Radius biometric server can be installed on the same machine as NAS. The server may use MS SQL 2000 database for biometric templates storage. MS SQL database makes it easy to import biometric data from BioBase. MS SQL database interface must then be applied to Radius server. The enrolment station can be established on a remote Windows 2000 system. The next subsections depict the scenario elements.

4.2. Biometric Client Terminal

A biometric variant of EAP (BEAP developed by Telefonica I&D, may serve as an example) can be enhanced with the Iris Module. This enables to adapt Iris Recognition Device with Radius client and consequently to setup a remote access scenario based on iris pattern analysis. The Iris Module has the following proposed functionality:

- It controls Iris Imaging hardware and captures iris images with the desired quality and speed,
- It processes the acquired images, i.e., a) detects the inner and outer iris boundaries within the raw camera image, b) localizes the eyelids and specular reflections, c) extracts two iris sectors based on the localized occlusions, d) transforms the iris sectors to the collection of *R* stripes,
- It calculates the biometric template based on the representation of the iris image as the sequence of signs of the Zak-Gabor expansion coefficients.

The Iris Module consists of the device library used for high-level hardware management and image capture, and the algorithms library, which deals with image processing, quality measurement, iris and occlusions detection, and features extraction functions. Figure 10 depicts the entire Client Terminal structure.

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

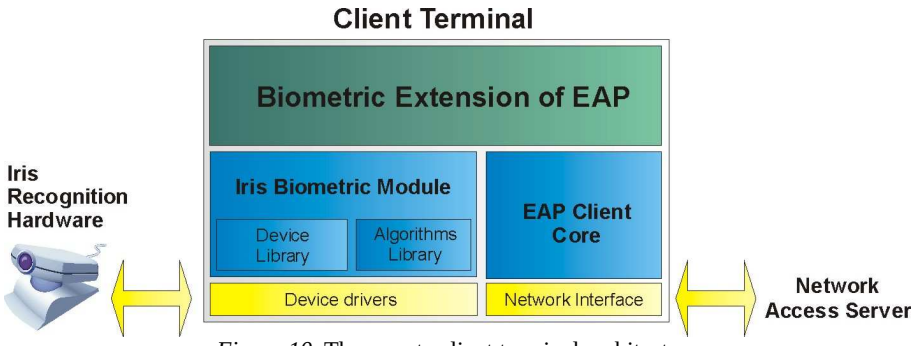

Figure 10. The remote client terminal architecture

4.3. Biometric Authentication Server

Radius server was configured to use MS-SQL BioBase server to store the templates. NASK BioBase Access Module add-on enables to make loading and storage of templates transparent to EAP Server Core. The server was also expanded by the iris matching algorithms, cf. Figure 11.

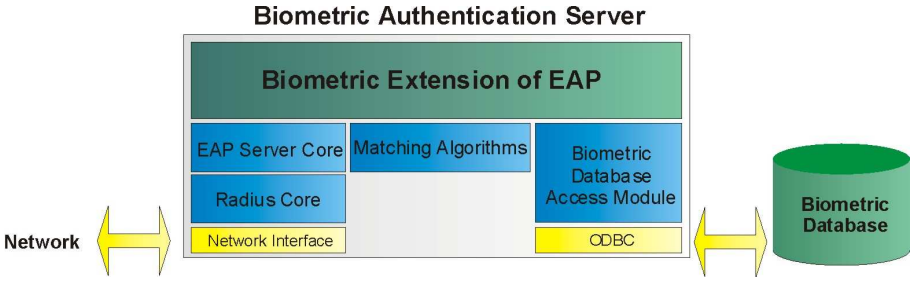

Figure 11. Biometric Authentication Server based on Radius servers, with remote Biometric Database

4.4. Enrolment Terminal

The Enrolment Terminal (cf. Fig. 12) uses the NASK Iris Module and BioBase Access Module. A separate application is developed that uses common elements of NASK biometrics modules, namely, the device library to control the hardware, and the algorithms library to process iris images and calculate iris features vectors.

The enrolment terminal captures a certain number of images of volunteer's eye. The raw image is processed to detect the inner and outer iris boundaries and eyelid occlusions. As an additional security mechanism, the occlusions may be used to determine volunteer-dependent free of occlusions

(FOC) angular iris sectors, used for iris code construction in place of pre-set angles. The FOC angles can enhance the iris code. The enrolment hardware helps the user to position his or head correctly behind the camera.

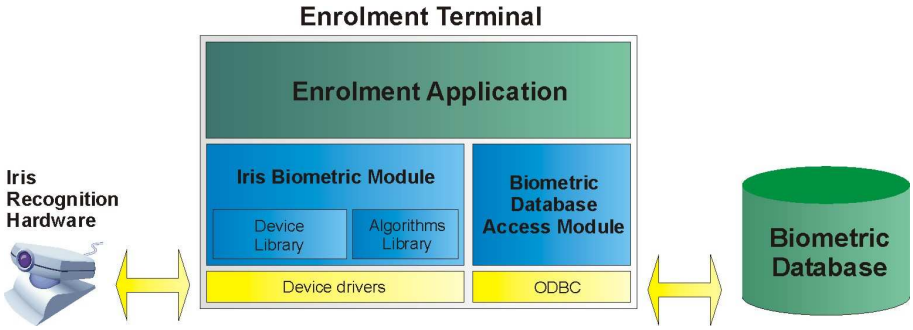

Figure 12. Iris biometrics enrollment terminal, developed at NASK for use with the remote access scenario

5. CONCLUSIONS

In the paper we described a new method of iris texture coding and feature extraction, together with its application to remote access security. We introduced the iris coding method based on Zak-Gabor coefficients sequence and the methodology of the optimal iris features selection. The proposed approach leads to zero false match and zero false non-match sample errors. We also showed how these ideas can be implemented in a secure remote access framework.

ACKNOWLEDGEMENTS

Most of the above results were obtained as a part of BioSec European integrated project IST-2002-001766.

REFERENCES

Iris recognition methods and devices

[A1] Flom and Safir, “Iris recognition system”, United States Patent 4.641.349, February 3, 1987

[A2] John Daugman, “Biometric identification system based on iris analysis”, United States Patent 5.291.560, March 1, 1994

[A3] Richard P. Wildes et al., “Automated, non-invasive iris recognition system and method”, United States Patent 5.572.596, November 5, 1996

[A4] Daniel Daehoon Kim et al., “Iris identification system and method of identifying a person through iris recognition”, United States Patent 6.247.813, June 19, 2001

[A5] Y. Zhu, T. Tan, Y. Wang, “Iris image acquisition system”, Chinese Patent Application No. 99217063.X, 1999

[A6] Y. Zhu, T. Tan, Y. Wang, “Biometric Personal Identification System Based on Iris Pattern”, Chinese Patent Application No. 9911025.6, 1999

[A7] Matsushita et al., „Iris identification system and iris identification method”, United States Patent 5.901.238, May 4, 1999

[A8] Doster et al., „Iris recognition apparatus and method“, United States Patent 5.956.122, September 21, 1999

[A9] Mann, et al., „System and method for aircraft passenger check-in and boarding using iris recognition“, United States Patent 6.119.096, September 12, 2000

[A10] McHugh, et al., “Handheld iris imaging apparatus and method”, United States Patent 6.289.113, September 11, 2001

[A11] Musgrave et al., “Iris imaging telephone security module and method”, United States Patent 6.377.699, April 23, 2002

[A12] W. W. Boles, B.Boashash, “A Human Identification Technique Using Images of te Iris and Wavelet Transform”, IEEE Transactions on Signal Processing, Vol. 46, No. 4, April 1998

[A13] Tan Tieniu, “Identity identifying method based on iris identification and its equipment”, State Intellectual Property Office of the People's Republic of China, No. 1282048, applicant: Institute of Automation, Chinese Academy of Science, January 31, 2001

[A14] Richard Patrick Wildes, Jane Circle Asmuth, Keith James Hanna, Stephen Charles Hsu, Raymond Joseph Kolczynski, James Regis Matey, Sterling Eduard McBridge, “Automated, non-invasive iris recognition system and method”, United States Patent US 5,572,596, assignee: David Sarnoff Research Center Inc., Princeton, N.J., USA, November 5, 1996

[A15] Adam Czajka, Andrzej Pacut, “Zak's transform for automatic identity verification”, Proceedings of the 4th International Conference on Recent Advances in Soft Computing RASC2002, 12-13 December 2002, Nottingham, United Kingdom, pp. 374-379, 2002

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005

Eye structure and anatomy

[B1] F. H. Adler, “Physiology of the Eye” St. Louis, MO: Mosby, 1965

[B2] H. Davson, “The Physiology of the Eye”, 2nd ed. Boston, MA: Little, Brown & Co., 1963

[B3] R.S. Snell, M.A. Lemp, “Clinical anatomy of the eye”, 2nd Edition, Blackwell Science, 1998

[B4] James P. Ivins, John Porrill, “A deformable model of the human iris for measuring small three-dimensional eye movements”, Machine Vision and Applications, vol. 11, str. 42-51, 1998

Time-frequency analysis

[C1] Denis Gabor, “Theory of communication”, Proc. Inst. Electr. Eng., Vol. 93 (III), pp. 429-457, 1946

[C2] Troy T. Chinen and Todd R. Reed, “A Performance Analysis of Fast Gabor Transform Methods”, Graphical Models And Image Processing, Vol. 59, No. 3, pp. 117-127, May 1997

[C3] Martin J. Bastiaans, “Gabor’s Expansion and the Zak Transform for Continuous-Time and Discrete-Time Signals”, w Josh Zeevi and Ronald Coifman (Ed.), Signal and Image Representation in Combined Spaces, pp. 1–43, Academic Press, Inc., 1995

[C4] B. Fisher, S. Perkins, A. Walker, E.Wolfart: Hypermedia Image Processing Reference, available online: http://www.cee.hw.ac.uk/hipr/html/hipr_top.html

[C5] S. G. Mallat, "Zero-crossing of wavelet transform", IEEE Transactions Information Theory, vol. 37, no. 14, pp. 1019-1033, 1991

[C6] Troy T. Chinen, “A Performance Analysis of Fast Gabor Transform Methods”, Graphical Models and Image Processing, Vol. 59, No. 3, pp. 117-127, 1997

Performance evaluation, standards

[D1] A.J. Mansfield, J.L. Wayman, “Best Practises in Testing and Reporting Performance of Biometric Devices”, NPL Report CMSC 14/02, August 2002

[D2] Common Criteria Biometric Evaluation Methodology Working Group, “Common Methodology for Information Technology Security Evaluation. Biometric Evaluation Methodology Supplement”, August 2002

[D3] Jim Cambier, “Biometric Data Interchange Formats – Part 6: Iris image data”, ISO/IEC 19794 Final Committee Draft

Andrzej Pacut, Adam Czajka, Przemek Strzelczyk, "Iris biometrics for secure remote access", in: J.S. Kowalik et al. (Ed.), Cyberspace Security and Defense: Research Issues, pp. 259-278, Springer, 2005