Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

Replay attack prevention for iris biometrics

Adam Czajka [*,**]
Member, IEEE
Adam.Czajka@nask.pl

* Research and Academic Computer Network NASK
Biometric Laboratories
Wawozowa 18
02-796 Warszawa
POLAND

Andrzej Pacut [*,**]
Senior Member, IEEE
A.Pacut@ia.pw.edu.pl

** Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warszawa
POLAND

Abstract - The paper presents an original, independent of typical cryptographic techniques, method of biometric replay attack prevention for iris biometrics. The proposed solution takes advantage of appropriate enhancements of iris templates and relies on appropriate data alteration within the image space resulting in significant changes of the resulting code in the iris feature space. Proposed methodology may be embedded into any non-reversible iris coding, yet in the reference implementation the authors propose to use an original Zak-Gabor-based iris coding. Minimal dependency between the iris image alteration procedure and the resulting iris template in Zak-Gabor coding enables transmitting the iris image alteration code and the resulting iris template even in a plan text without lessening the system's security. The BIOBASE iris image database, as collected in NASK Biometric Laboratories, was used for the method development. The proposed methodology was evaluated with a body of different image alteration codes and with the use of the largest publicly available database from BATH University – DB 1600. The results prove the high potential of the method.

Index Terms — biometrics, replay attack prevention, iris recognition.

I. INTRODUCTION

The enhancement of identity authentication systems with biometric data verification brings potential risks resulting from the nature of biometrics. One of the weak application of biometric based verification is a remote access scenario, where biometric data (in any form) must travel over distrusted media. Since biometric data is difficult to change (unlike passwords), each transfer of sensitive data is typically associated with the justified concern of data theft. Once biometric data is stolen, it may (theoretically) be reused by a thief in illegal authentication transactions. Such illicit use of valid biometric data is called *biometric replay attack* (BRA). This type of attacks is distinguished from the more general *replay attack*, where the nature of the stolen data is not defined. We do not consider illegal presentations of objects (artificial or alive) to the biometric sensors as BRA since the principles of such attacks are not based on a replay transmission of eavesdropped biometric data. Such attacks are subject to aliveness detection methodology [1,2].

The BRA is often addressed in biometric discussions, however, to the best knowledge of the authors, there are no systematically developed and published reliable BRA prevention methods for the iris. Commercially available products use common cryptography routines to prevent the iris templates from spoofing, by joining the code with a nonce, and additionally encrypting the resulting package. Although this procedure is theoretically able to prevent BRA, it relies on secrets (e.g. encryption keys) that must be kept and exchanged securely besides the biometric templates. Each secret is prone to be compromised, and once concluded, the biometric template is open to interception, since typically no additional BRA prevention is applied.

Special enhancements of biometric templates makes it possible to develop specialized BRA prevention methods. Daugman suggests [2] modifying the *IrisCode*™ to prevent the system from BRA, yet the proposition is not implemented and examined. The enhancement relies on permutations of the code bytes, thus resulting in permuted binary sequences still referring to the same eye. Although the number of possible permutations is relatively large (for 256-byte code this is $256! \approx 10^{506}$), this concept has its disadvantages. Namely, both transaction parties must possess the same permutation key, and thus the secret must be exchanged securely. Each time the transaction is accomplished, the permuted sequence travels over the distrusted medium. Each permuted sequence contains information on the entire set of iris features. Once the secret is compromised, a single observation is required to ascertain the original *IrisCode*™.

The authors propose a BRA prevention method that relies on *randomized iris sectors*, thus moving the permutation issue from the feature space (as in Daugman's suggestion) to the iris image space. This approach constructs the iris template being self-contained with regard to BRA prevention. Since the Zak-Gabor-based coding [4] is used in this reference implementation, we briefly present the most important principles of this coding in the next Section.

II. ZAK-GABOR-BASED CODING

The iris coding aims at designating a set of local iris features to form a compact image representation. Raw image of the eye contains many elements that obstruct recognition (eyelashes, eyelids, light reflexes etc.). The image undergoes the process of localization of occlusions and two iris sectors

Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

free from occlusions are selected. Iris sectors are converted to a series of *iris stripes*, Figure 1. The number (R=32) and the length (P=512) of each iris stripe is identical to either eye, regardless of the degree of dilation of the pupil and the scale of the object within the image.

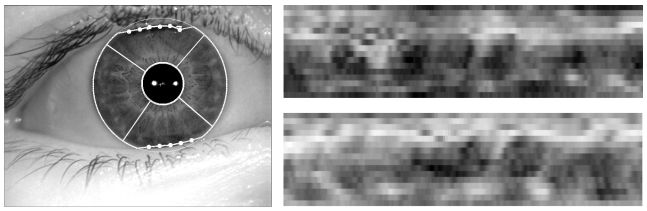

Figure 1. Iris image with occlusions detected (left) and iris stripes (right)

We use Gabor expansion to represent each iris stripe f_l l=0,...,R-1, namely

$$f_\ell(p) = \sum_{m=0}^{M-1} \sum_{k=0}^{K-1} a_{mk;s\ell} g_{mk;s}(p), \quad p = 0 \dots P-1 \qquad (1)$$

where

$$g_{mk;s}(p) = g_s(p - mK) e^{ikp2\pi/K}, \quad p = 0 \dots P-1 \qquad (2)$$

is shifted and modulated version of elementary function

$$g_s(p) = e^{-\pi \left((p+\frac{1}{2})/2^s\right)^2} \qquad (3)$$

and s=2,...,8, k=0,...,K-1, m=0,...,M-1 and MK=P. The Zak transform is used to calculate Gabor's transformation coefficients $a_{mk;sl}$. Zak's transform is considered as the fastest and the most accurate method for calculation of Gabor's expansion coefficients. We use signs of Gabor's expansion coefficients a as the iris features $\mathbb{B}$, namely

$$\mathbb{B} = \{\mathrm{sgn}(\Re(a_{mk;s\ell})), \mathrm{sgn}(\Im(a_{mk;s\ell}))\} \qquad (4)$$

Fisher's information related to the transformation coefficients was analyzed on the development database of iris images and the number of elements in $\mathbb{B}$ (hence bits) is 1024. The order of features is kept identical for all images. Thus, the matching between irises requires only the XOR operation between two feature sets, and the Hamming distance is applied to calculate the score ξ, namely

$$\xi = \frac{1}{N} \sum_{n=0}^{N-1} (b_n^{(1)} \ \mathrm{XOR} \ b_n^{(2)}) \qquad (5)$$

where $b^{(i)}_n$ is the n-th bit of i-th sample and N=1024 is the number of iris features. Factor $1/N$ makes $\xi \in \langle 0,1 \rangle$.

We stress that $\mathbb{B}$ should not be confused with the so called *IrisCode*™ invented by Daugman [3]. The latter one is a product of an iris image filtering, while $\mathbb{B}$ is derived from Gabor expansion coefficients.

The use of coefficients rather than Gabor's filtering, which is typically used in commercial systems, has many advantages, e.g. limited dependency between an iris image and a code has a particular value when embedding the replay attack prevention mechanism.

III. RANDOMIZED IRIS STRIPES

A method of biometric replay attack prevention based on employing certain characteristics of the applied iris coding is detailed below. While Zak-Gabor's transform is *reversible*, by neglecting the exact values of coefficients, Zak-Gabor-based coding is made *non-reversible*, i.e. once the iris features (i.e. bits in $\mathbb{B}$) are known, there is no possibility to reconstruct the iris stripes (thus the original iris image). Randomization of parts of iris stripes results in constructing a representation of a *de facto* new, possibly inexistent, iris. Representation of the artificial iris, like any digital image, may still be transformed into code using Zak-Gabor-based coding. Since there is no possibility to reconstruct the original iris stripes, the eavesdropper has a very limited chance predicting the correct code required for the next verification, even if the corresponding permutation key send by the server is known to him. This, in turn, is possible when the randomization is performed in the feature space, as proposed earlier [2]. It will be shown that the calculation of a valid feature set requires both the permutation key and the iris image.

It is assumed that the permutation is performed independently within each stripe. Thus, each l-th stripe (l=0,...,R-1) is cut into parts which are called *striplets*, see Figure 2.

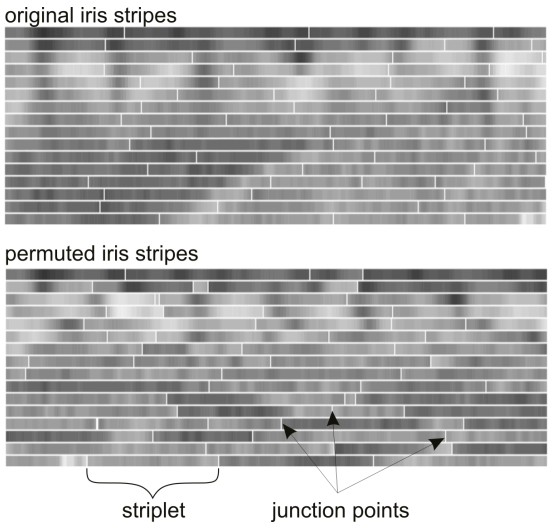

Figure 2. Iris stripe permutation. The original iris stripes are independently cut into striplets, shown in the top image. The resulting permuted iris stripe collection is shown in the bottom image.

Permutation of striplets requires recalculating the iris template each time the verification is needed, both on the server and the client hosts, using the same known rule. This poses special processing demands to the coding algorithms, and such real-time template recalculations are possible to achieve if efficient iris coding algorithms are applied. The author's implementation of the Zak-Gabor-based coding calculates iris features within approximately 60ms on a PC workstation for all iris stripes, and this is recognized as sufficient speed. This biometric attack prevention approach requires iris stripes with corresponding sector angles to compound the iris template, instead of the calculated codes.

The allowed width of each striplet is set experimentally

Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

(from 1/8 to 1/4 of the stripe width), to prevent the method from cutting stripes inappropriately, since too large and too small striplets do not differentiate bits of the resulting code sufficiently. Once the striplets are generated, the routine permutes the striplets independently within each stripe. This leads to the representation of an iris whose structure is different from the original one. Figure 2 illustrates the cutting of the iris stripes into striplets and the resulting permuted representation.

IV. EVALUATION OF RELIABILITY

To illustrate the reliability of this method, comparisons between same eye images and different eye images were made for iris images originating from two sets: BIOBASE [5] and BATH DB1600 [6].

Since each feature set $\mathbb{B}$ is strictly associated with a particular permutation key, four recognition variants are examined:

1. Iris features are determined for different images of the *same* eye, rearranged according to the *same* permutation key. This situation is typical for regular verification. This case is marked as **SESK** (Same Eye – Same permutation Key).
2. Similar to 1, but iris striplets are permuted with *different* permutation keys. This situation is typical when a known iris image is altered with an inappropriate permutation key. This case is marked as **SEDK** (Same Eye – Different permutation Key).
3. Iris features are determined for *different* eyes but rearranged using the *same* permutation key. This situation matches typical impostor trial using a wrong eye and eavesdropped permutation key. This case is marked as **DESK** (Different Eye – Same permutation Key).
4. Same as DESK, but striplets are rearranged with *different* permutation keys. This scenario is typical when both the permutation key and iris stripes are unknown, yet impostor comparison is carried out. This case is marked as **DEDK** (Different Eye – Different permutation Key).

For each dataset, I=3 iris images were chosen randomly for each eye and the enrollment process was performed to check whether selected images are of sufficient quality to be used in BRA prevention reliability evaluation. Not all images among those available in the datasets passed the enrollment procedure, and we could enroll J_{BIOBASE}=180 and J_{BATH}=1464 different eyes registered in BIOBASE and BATH DB1600, respectively.

The spontaneous eye rotation angle which always exists in one-eye imaging systems is compensated with the use of correlation method [4], in order not to disrupt the effects related to striplets permutation. A total of v=38 random permutation keys were generated. For same-eye comparisons (SESK and SEDK cases), comparisons among all pairs of all I images were made. For different-eye comparisons (DESK and DEDK) within the BIOBASE images, one image pair was generated for each permutation key and for each combination of different eyes. Due to relatively large number of eyes registered in BATH DB1600 database, the number of different-eye comparisons (DESK and DEDK) was narrowed, and for each eye u=3 different eyes were randomly chosen to generate u impostor pairs of images. Table 1 gives the appropriate formulas and provides the numbers of comparisons prepared for each recognition variant and each database used.

TABLE I
NUMBERS OF COMPARISONS MADE FOR EACH RECOGNITION VARIANT AND DATABASE USED

	BATH DB1600	**BIOBASE**
SESK	vIJ_{BATH} = **166 896**	vIJ_{BIOBASE} = **20 520**
SEDK	$v(v\text{-}1)IJ_{\mathrm{BATH}}/2$= **3 087 576**	$v(v\text{-}1)IJ_{\mathrm{BIOBASE}}/2$ = **379 620**
DESK	uIJ_{BATH} = **166 896**	$vJ(J\text{-}1)/2$ = **612 180**
DEDK	$uv(v\text{-}1)J_{\mathrm{BATH}}/2$ = **3 087 576**	$v(v\text{-}1)J_{\mathrm{BIOBASE}}(J_{\mathrm{BIOBASE}}\text{-}1)/4$ = **11 325 330**

Figures 3-10 show the distributions of comparison scores for different recognition variants. The distribution for SESK (Figs. 3 and 7), i.e. that obtained when the same permutation keys are used, leads to the average score of 0.195 (BATH DB1600) and 0.123 (BIOBASE) and is highly different from those scores obtained for either different eyes or different permutation keys, namely for BATH DB1600: 0.468, 0.473, 0.481 and for BIOBASE: 0.489, 0.469, 0.493 for SEDK, DESK and DEDK, respectively. The scores achieved for different permutation keys are comparable to those observed when different eyes are compared.

Analyzing in detail the average comparison values it may be concluded that the existence of junction points has the first priority in shaping the distributions of scores. For BIOBASE samples both DEDK and SEDK, and thus cases when different permutation keys are used, depict comparable average comparison results (Figs. 4 and 6), although the DEDK case is slightly closer to the theoretically ideal case of scores equal to 0.5. This slight difference in scores is caused by making comparisons between different eyes in the DEDK case and between the same eyes for SEDK. In turn, results obtained for DESK (the same permutation keys applied to different eyes) differs by approximately 0.03 (score distance) from the theoretical 0.5, thus moving the DESK distribution left in comparison to the cases when different keys are employed. This is due to the discontinuities in iris stripes that are located in identical places for DESK. These abrupt changes to iris stripe functions may prevail over iris intensity fluctuations and may leverage the similarity between the compared data, even if originating from different eyes. However, this phenomenon still makes it very difficult to perform correct verification with the use of eavesdropped permutation keys and inappropriate iris stripes.

Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

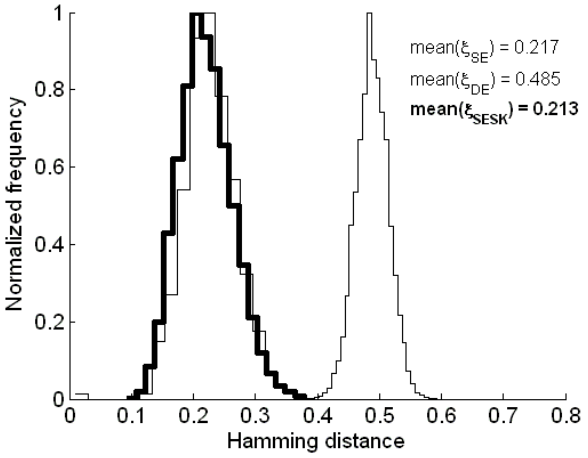

Figure 3. Distributions of comparison scores for same (ξ_{SE}) and different (ξ_{DE}) eyes calculated with the use of BIOBASE set of images. Distribution of comparison scores for SESK variant is shown in bold.

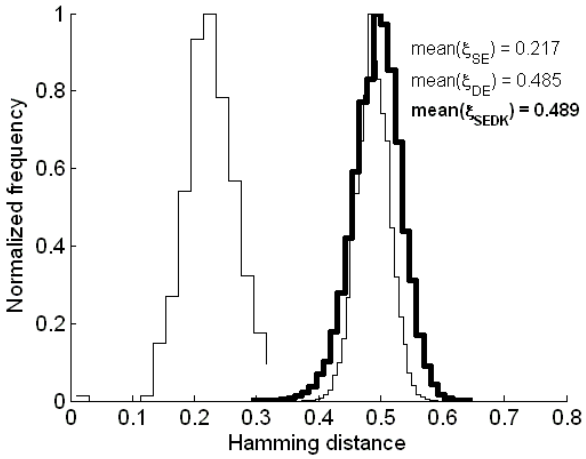

Figure 4. Same as in Fig. 3 but the distribution of comparison scores for SEDK variant in shown in bold.

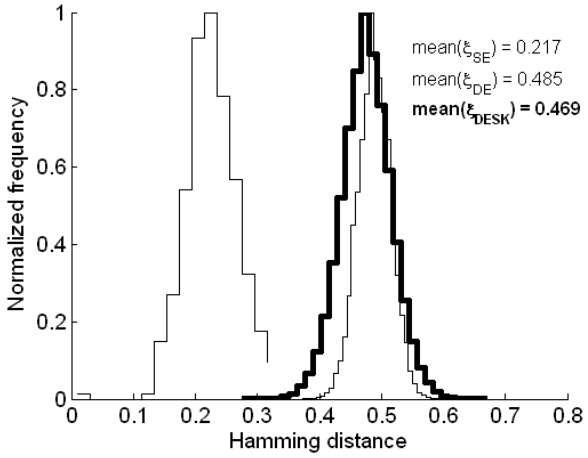

Figure 5. Same as in Fig. 3 but the distribution of comparison scores for DESK variant in shown in bold.

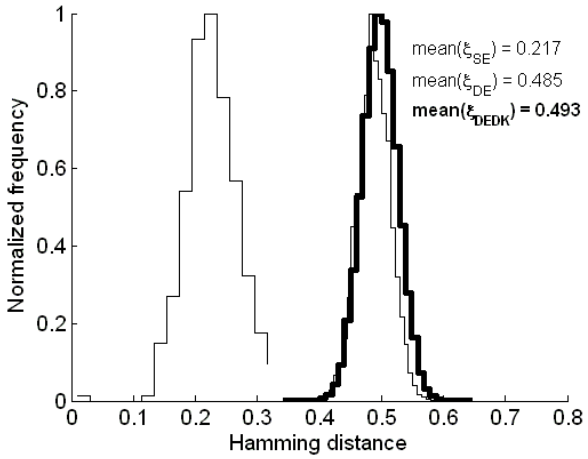

Figure 6. Same as in Fig. 3 but the distribution of comparison scores for DEDK variant in shown in bold.

For BATH DB1600 samples the average comparison values for DEDK, SEDK and DESK variants are similar to the average comparison value between non-altered different irises. The BIOBASE samples were used to develop the Zak-Gabor-based coding and the presented BRA prevention methodology, and thus inserting fake frequencies (i.e. resulting from stripe permutations) influences the estimation results (i.e. calculated with the use of BIOBASE) to a higher extent that for testing results (i.e. calculated with BATH DB1600 set of images).

Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

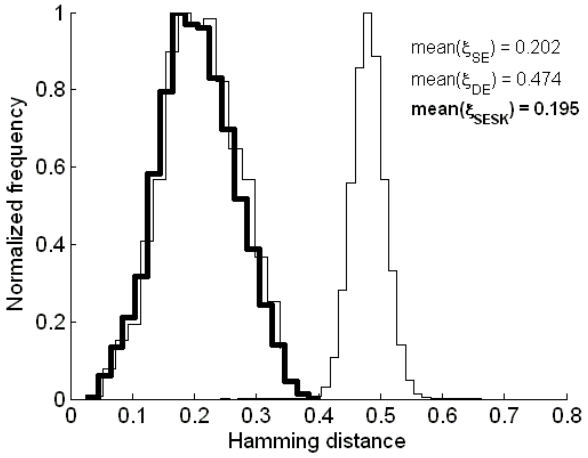

Figure 7. Same as in Fig. 3 but distributions calculated with the use of BATH DB1600 set of images are shown.

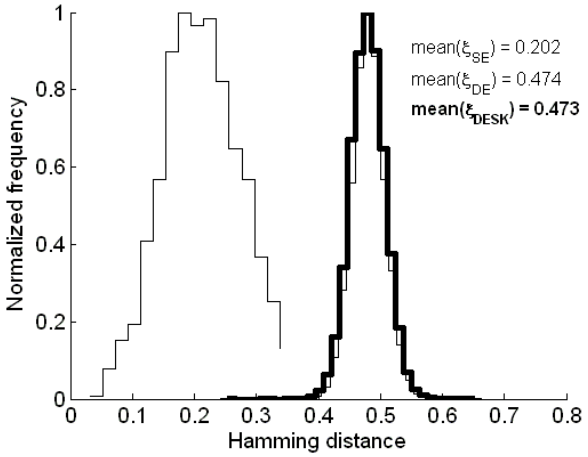

Figure 8. Same as in Fig. 7 but the distribution of comparison scores for DESK variant in shown in bold.

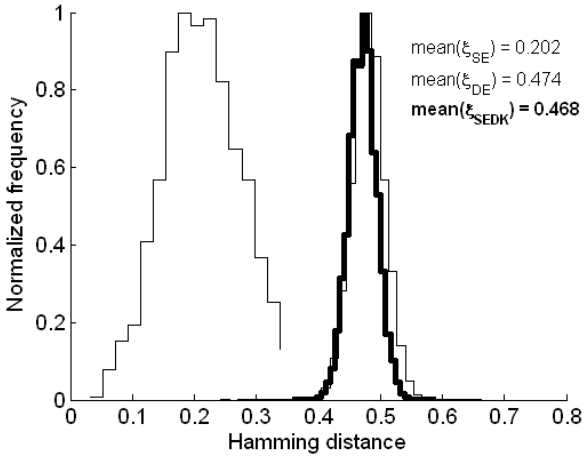

Figure 9. Same as in Fig. 7 but the distribution of comparison scores for SEDK variant in shown in bold.

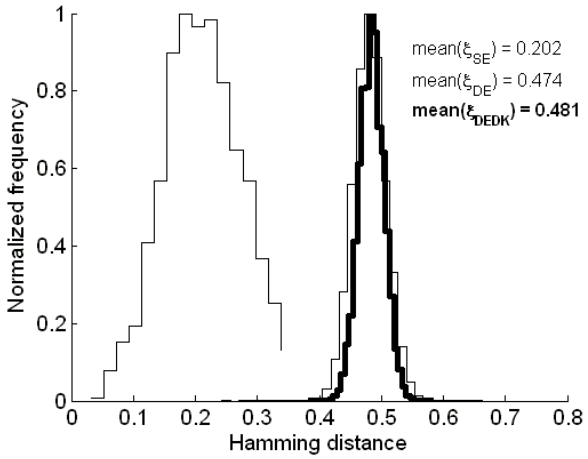

Figure 10. Same as in Fig. 7 but the distribution of comparison scores for DEDK variant in shown in bold.

Tables II and III present the equal error rates for iris recognition systems built according to different template generation rules. We may observe that EER values are slightly higher in the proposed scenario with stripes permutation, however they still remain on acceptable low levels and show that the mandatory information for correct verification is both the biometric data and the appropriate permutation key. Missing any element out of these two may lead to wrong identification.

TABLE II
EQUAL ERROR RATES (%) FOR RECOGNITION SYSTEMS BUILT ACCORDING TO DIFFERENT IRIS TEMPLATE GENERATION RULES CALCULATED FOR BIOBASE SET OF IMAGES. THE MOST INTERESTING VALUES ARE MARKED IN BOLD FACE.

	DE	**SEDK**	**DESK**	**DEDK**
SE	**0**	0.0134	0.0206	0
SESK	0.0095	**0.1653**	**0.2075**	**0.0101**

TABLE III
SAME AS IN TABLE II EXCEPT THAT THE BATH DB1600 SET OF IMAGE IS USED.

	DE	**SEDK**	**DESK**	**DEDK**
SE	**0.0017**	0	0.0021	0
SESK	0.0230	**0.0111**	**0.0315**	**0.0014**

One of the advantages of this procedure over the method that alter only the iris features is that a theft of the permutation key is not dangerous. The key dictates changes within the secret (located within the iris images space) and in consequence changed data are coded by the non-reversible transform into binary sequence (iris features space). The aim of a spy in this case is to learn how to generate the appropriate code that corresponds to the server request (permutation key). The effect of this learning, however, must finally become the original iris data (iris stripes), since only the knowledge of the iris image original fluctuations allows generating codes that are expected by the server. Note that the secret (iris stripes) or its part is never sent. Thus, multiple observations of the compromised transmission channel do

Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

not lead to the acquisition of data allowing one to predict appropriate iris features having a valid permutation key.

Embedding this concept into the iris coding methods based on image filtering is also possible. However, in such coding, elements of the resulting code correspond to particular iris areas. The permutation discussed here and the resulting code may thus have stronger correlations like in the method based on Zak-Gabor's coefficient coding.

V. IMAGES, CODES AND THEIR INTERACTIONS

Developing the BRA prevention methodology by alteration the original iris images provides some interesting observations related to iris images and features (codes) and their mutual interactions. We summarize them in the following section.

Due to the nature of the Zak-Gabor-based coding, there is a possibility of generating images of "artificial irises" (possibly having no counterparts in live organs) that result in an identical feature set $\mathbb{B}$. This is true also for coding employing image filtering, due to loss of information while coding the response of the Gabor filters. Furthermore, the theoretical number of possible "artificial irises" showing an identical code is infinite. It may be further concluded that the famous sentence "no two irises have the identical code", often accompanying the presentations of the Daugman's method [3], may be overestimated.

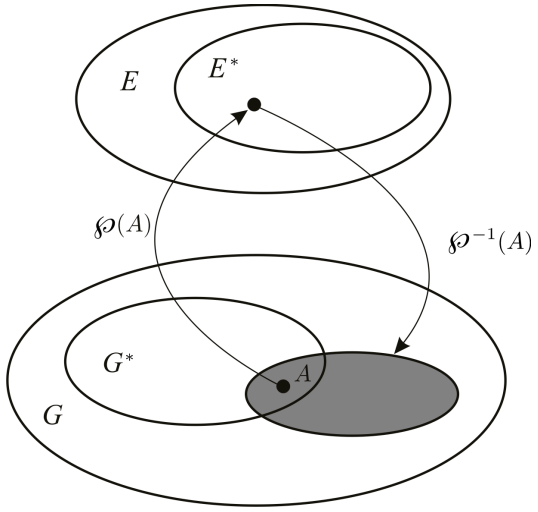

Figure 11. Images and binary codes as separate spaces. This illustrates that there **is** a possibility to generate two different images, possibly having no counterparts in live irises, that result in identical iris feature set.

Figure 11 illustrates the problem addressed in the above paragraph. Consider the space G of all gray-scale images of appropriate dimensions. This space is the most general, and in particular it encapsulates a subspace of live iris images G^*. Similarly, let E denote the space of binary sequences of appropriate length, which includes a subspace E^* of iris codes. Any gray-scale image, shown as point A, can be mapped to the corresponding code $\wp(A) \in E^*$. We believe that the Hamming distance between $\wp(A)$ and $\wp(B)$ for any two different irises A and B is sufficiently large to guarantee zero error rates for the chosen acceptance threshold. However, when the number of possible elements in the corresponding spaces is investigated, it may be concluded that there must be more than one image mapped to the same code. Indeed, assuming N-bit codes, there are 2^N elements in E^*. In turn, in the space G^* there are 2^{8RP} possible gray scale images of the size $R \times P$. In this work, N=1024, R=32 and P=512, hence $2^N << 2^{8RP}$. The set of images resulting in the same code $\wp(A)$ is denoted by $\wp^{-1}(A)$. Any image $C \in \wp^{-1}(A)$ may not resemble the image of a live iris due to significant departures from the iris tissue morphology. However, one may hypothetically add morphology rules to the texture generation routine, and narrow $\wp^{-1}(A)$ to produce only artificial iris images. Such a situation seems to be ignored by Daugman.

The conclusion is that it is not possible to guarantee that every two irises have different codes, both coding the iris using image filtering and the Zak-Gabor-based approach. Thus, it is recommended to proceed carefully when injecting artificial irises into the system. By striplet permutation, stripes constructed possibly do not reflect the fluctuations observed in real iris images. If the presented biometric replay attack is employed for a large population to identify (not to verify) an individual, there is a danger of creating such an "artificial iris" that corresponds to more than one subject. Consequently, to limit these occurrences, the iris striplet permutation is narrowed only to stripes, and striplets are not permuted in a radial direction.

VI. REFERENCES

[1] Andrzej Pacut, Adam Czajka, "Aliveness detection for iris biometrics", *2006 IEEE International Carnahan Conference on Security Technology, 40th Annual Conference, October 17-19, Lexington, Kentucky*, IEEE 2006

[2] John Daugman, "Anti-spoofing", available on-line (March 2005): `http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf`

[3] John Daugman, "How Iris Recognition Works", *IEEE Transactions on circuits and systems for video technology*, Vol. 14, No. 1, January 2004

[4] Adam Czajka and Andrzej Pacut, "Iris Recognition with Adaptive Coding", *Rough Sets and Knowledge Technology*, Lecture Notes in Artificial Intelligence, Vol. 4481, pp. 195-202, Springer, 2007

[5] BIOBASE Multimodal Biometric Database, `http://www.BiometricLabs.pl`, Biometric Laboratories, NASK, 2003

[6] University of Bath Iris Image Database, `http://www.irisbase.com`, 2007

VII. VITA

Andrzej Pacut, Ph.D, D.Sc. - received his M.Sc. in Control and Computer Engineering in 1969, Ph.D. in Electronics in 1975, and D.Sc. in Control and Robotics in 2000. Since 1969 he is with Warsaw University of Technology, being a Professor in the Institute of Control and Computation Engineering. Since 1999 he is with Research and Academic Computer Network NASK. He was Visiting Prof. at the Lefschetz Center for Dynamic Systems at Brown University, Providence, Rhode Island 1980–1981, and Visiting Prof. in

Adam Czajka, Andrzej Pacut, „Replay attack prevention fpr iris biometrics", Proceedings of the 42nd Annual 2008 IEEE International Carnahan Conference on Security Technology, October 13-16, 2008, Prague, Czech Republic, pp. 247-253

the Department of Electrical and Computer Engineering of Oregon State University, Corvallis, Oregon, 1986-1991. He is a senior member of the IEEE, a member of INNS, and serves as the President of the IEEE Poland Section. He is a member of the NASK Research Council and the head of the NASK Biometric Laboratories.

Adam Czajka, Ph.D. - received his M.Sc. in Computer Control Systems in 2000 and Ph.D. in Control and Robotics in 2005 from Warsaw University of Technology. Since 2003 with WUT, and since 2002 with Research and Academic Computer Network (NASK). He is a member of the NASK Research Council (2006-). Member of Polish Committee for Standardization (*Technical Committee 182 - Information Security in IT Systems*, 2007-). He is also a member of the IEEE (2002-) and serves as the Secretary of the IEEE Poland Section (2005-).