Information-Theoretic Analysis of Iris Biometrics for Biometric Cryptography

Sasa Adamovic, Milan Milosavljevic, Mladen Veinovic, Marko Sarac, Aleksandar Jevremovic

Department of Informatics and Computing, Singidunum University
32 Danijelova Street, 11000 Belgrade, Serbia
(sadamovic, mmilosavljevic, mveinovic, msarac, ajevremovic)@singidunum.ac.rs

Abstract: This paper presents a rigorous information-theoretic analysis of iris biometrics with the aim to develop optimized biometric cryptosystems. By estimating local entropy and mutual information, we identify the iris regions that are most suitable for these purposes. Parameter optimization of the appropriate wavelet transform produces higher entropy and low mutual information in the transformation domain. This establishes an effective framework for the development of systems for the extraction of truly random sequences from iris biometrics, while not compromising its proven authentication features.

Keywords: iris biometrics; image analysis; information theory; image texture; biometric cryptosystems

1 Introduction

According to some estimates, the entire field of information protection should make a radical qualitative leap and a shift of the fundamental paradigm of computer security towards a paradigm of information-theoretic security [1]. Such a shift would allow the creation of an entire class of cryptographic mechanisms whose compromisation would be independent from the attacker's computing power. All this points to a new position of this discipline within the general theory and practice of information protection systems. Information analysis of source biometric data is crucial for construing concrete solutions of a biometric cryptosystem with a theoretically guaranteed performance rate.

Biometrics has established itself as a significant source of cryptologic parameters in the domain of reliable and practically acceptable authentication. Biometric systems are based on physical and behavioral characteristics of human beings such as fingerprint, voice, face, iris and others. The strength and resistance of these systems are directly related to the natural amount of information present in a biometric source. In order to estimate the maximum quantity of information, one

must have a good understanding of biometric data specific to a particular source, as well as the technology used to precisely read and extract information.

The original concept of "Biometric encryption" was applied to fingerprints in 1994. The pioneer in this area is Dr. George Tomko, the founder of Mytec Technologies, Toronto, Canada. Ever since, numerous researchers have contributed to this and other related technologies. Besides the Biometric Encryption, the term biometric cryptosystems is also used. We shall use the abbreviation "BC" in the remainder of this text to denote biometric cryptosystems. Generating keys for various cryptographic purposes based on biometric data is an important idea. A prime example of one such system is given in [2], where authors achieve a promising result (FRR (false rejection rate) = 0,47%, FAR (false acceptance rate) = 0%, key length = 140 bits) in an iris biometry application. This system enables a multipurpose use of a biometric template, without the possibility of compromisation. This result opens a door to a wide application in cryptographic protection mechanisms. Furthermore, the authors carried out the analysis of noise and errors that occurred while forming the iris biometric template. Pertaining results enabled them to select an adequate code, which is optimized with regard to the maximum allowed capacity determined by the iris biometric source. A 2D Gabor wavelet was used to extract 2048 bits of phase information which produces approximately 249 degrees of freedom [3].

Most BC systems applied to a variety of biometric characteristics produce fairly long keys (140 bits [2], 186 bits [4], 240 [5] bits). This imposes the following question: what is the true quantity of consistent information available within biometric data, based on which it is possible to generate a cryptographic key? This very information serves as the material for key generation. In that case, the key itself cannot be longer than the quantity of biometric information. If this were to happen, it would only speak of overly high performance settings for the debugging code, which inevitably leads to FAR being greater than zero. In addition to acceptable FRR values, algorithms suggested by the majority of authors [4, 5, 6, 7] have FAR values greater than zero percent. From our point of view, practical application of such BC systems is unacceptable. Also, other algorithmic solutions [2, 8, 9, 10] were proposed that result in both FAR being equal to zero percent and FRR having acceptable values. However, it remains to be determined whether those solutions fully utilize the true capacity of the system and to identify the system's maximum level of effectiveness [11].

Considering the above-stated, we assume that a strong information-theoretic foundation and the application of the Theory of Perfect Cyphers are indispensable for successfully developing BC systems. The theory was proposed by Shannon [12]. The information-theoretic analysis of biometrics, as a special information source, would provide concrete solutions for development of BC systems with theoretically guaranteed performance.

This paper is concerned with a rigorous information-theoretic analysis of iris. We apply measures of information (entropy, local entropy, and mutual information) to identify iris regions that are most suitable for generation of cryptologic keys. Also, optimization of the parameters of the transform function produces higher entropy and reduced mutual information in the transformation domain. This establishes the foundation for development of a BC system for estimation of truly random or consistent bits from the iris biometric source. In addition, the authors are concerned with the complex procedure of processing iris biometric data [13]. Biometric data contains various types of noise that may significantly increase the degree of variability, which further alters the quality of information obtained.

The remainder of this work is organised as follows. The next section discusses the biometric database used, which is followed by a detailed information-theoretic analysis consisting of calculating local entropy over a texture of iris image after the normalization phase, determining optimal parameters in the transformation domain (iris coding phase), modeling of the iris information source by means of Shannon approximation models, measuring mutual information between identical and different irises, and the setup of an information-theoretic foundation for iris biometrics. The final section comprises the conclusion and an overview of the contributions of our work.

2 Information Analysis and Experimental Results

We used the CASIA Iris Image Database version 4.0, for the experimental portion of our work. This database was created by researchers from the Institute of Automation, Chinese Academy of Sciences, and it contains several thousand iris images [14]. Several versions of the database were offered free of charge to the international biometric research community. Over 4000 users from 70 countries have downloaded the CASIA database so far and a vast number of researchers have used it in their work.

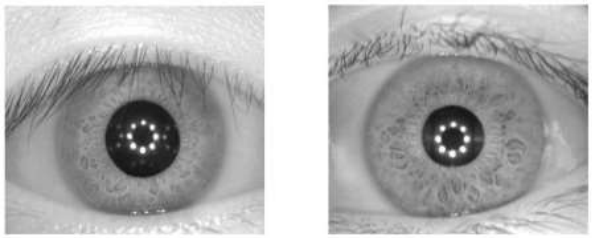

Figure 1
Samples of iris images from the CASIA-Iris V4 database

Fig. 1 provides test samples of iris images in the gray-scale format, acquired by means of special cameras.

2.1 Analysis of Iris Image Texture

In the first part of the information analysis we measure the entropy of an iris texture image after the normalization phase. The number of iris rings is 20 with 240 points on each. By means of the Daugman's rubber sheet [15] model, we obtain a gray-scale image with a resolution of 20 x 240 pixels. Pixel depth is 8 bits, whereby each pixel is represented by a gray shade from the 0 to 255 range of decimal values. Fig. 2 depicts the normalization process and the resulting rectangular iris texture.

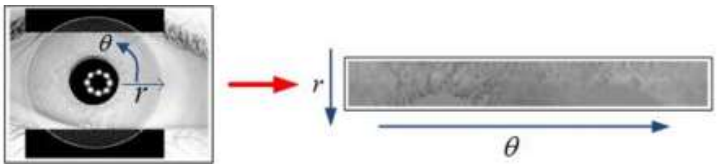

Figure 2
Iris texture in the first phase

In the next step, we calculate the local entropy over the iris texture we obtained in the manner described above. Due to the nature of data, we employed the method commonly used to determine the entropy of two-dimensional signals [16, 17]. This method essentially utilizes the Shannon entropy [18]. Entropy is most conveniently defined as an average quantity of information or the measure of uncertainty of an information source (iris, in our case). For a known probability p, entropy of an event is calculated by:

$$H = -\sum_{i=1}^{l} p_i \log_b p_i \quad (1)$$

where p_i pertains to symbol probabilities obtained through image histograms.

The value of local entropy varies based on the chosen window size. The window is square-shaped and it represents the number of included neighboring pixels. The values obtained are represented by means of a binary logarithm, where 1 bit is the unit of quantity of information. The chosen method allows for the use of a varying number of neighboring pixels, which is quite similar to Shannon's approximation models – the concept used in modeling natural language as an information source.

Fig. 3 depicts a 3D model of local entropy for the chosen windows size of 9x9. The model represents average local entropy values for each individual pixel position. The illustration reveals that the first circular iris region (next to the pupil) has a larger local entropy. This is clearly seen on the y-axis that displays the quantity of information (i.e., achieving 5 bits per pixel out of the maximum possible 8 bits per pixel). Also, a closed circular contour in the X, Z, clearly points out to the higher entropy region. The average local entropy in this experiment differs significantly in the first (4.4412 bits per pixel) and the second region (3.6020 bit per pixel). Based on the results obtained, we adopt the division of iris by regions whereby the first region becomes the primary interest of our research.

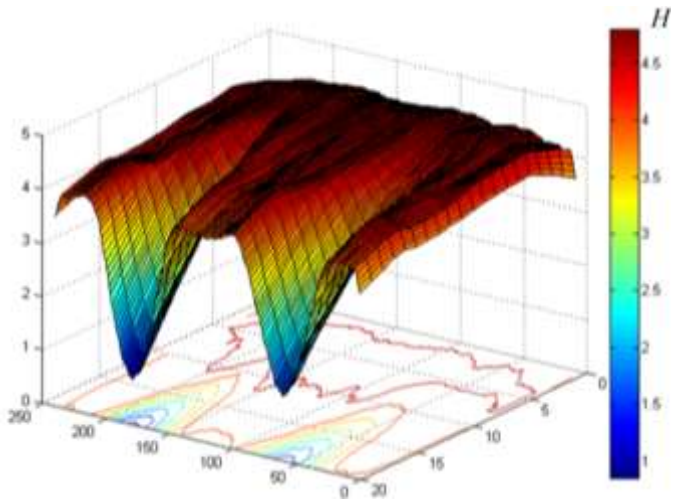

Figure 3
A 3D information model of local entropy (CASIA Iris Image Database version 4.0)

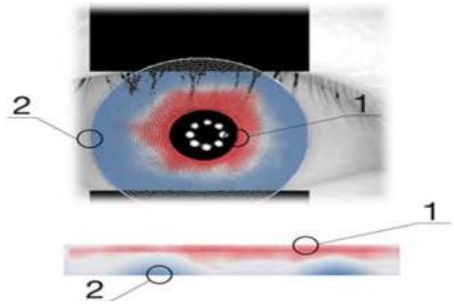

Figure 4
Division of iris by regions (red color (1) - higher information value, blue color (2) - lower information value)

Fig. 4 illustrates the first region of iris, determined to be of higher information value, whereas the second region is characterized by a decline of quality as measured by local entropy.

Low quality of the second region is attributable to eyelids and lashes, but also the automatic segmentation phase where algorithms do not attain 100% accuracy. Regardless of the shortcomings, we observe that both the left and the right side of the iris in the second region have lower entropy (area not covered by eyelids and lashes). Therefore, the second region cannot be used to extract material for generating cryptologic parameters. Moreover, due to the impreciseness of segmentation algorithms, practical applications of BC systems lead to higher FRR parameters. Researchers attempt to remedy this problem by designing various concatenated security codes that often lead to FAR values greater than zero percent.

2.2 Analysis of Optimal Parameters in the Transform Domain – Iris Coding

We conduct the next information analysis on a biometric iris template code or iris information source following the coding phase. There are several important parameters for the algorithm utilized in the coding phase. This phase results in an iris biometric template. The success of this phase depends on the optimal choice of parameter values used to provide high entropy of the iris code and the maximum possible quantity of consistent bits. The following comparative analysis was carried out in the part of the process where iris code is formed. In fact, by analyzing the biometric template – iris code, we conduct an analysis over the iris information source.

The parameters of interest include radial and angular resolution (r and θ); in other words, the parameters that produce the number of points in the iris image that will be coded in each iris, as well as filter parameters used to extract only unique iris characteristics. Filter parameters include: filter number N, wavelength λ_n (in pixels), bandwidth given as σ/f, and the multiplicative factor between center wavelengths of successive filters α.

It is known that altering the wavelength parameter $\lambda_n$of the filter provides the opportunity to increase the entropy of the source and the number of consistent bits. For an in-depth discussion and technical details please see [19] and [20].

Figure 5
Biometric template – binary iris code

Fig. 5 shows an example of the iris code (in binary format) with masked portions of iris code that contain errors caused by eyelashes and lids. The following results were obtained using a methodology similar to that applied in the preceding information analysis. We analyzed iris code at the binary matrix level over which we calculated local entropy. The dimension of the iris code after the coding phase is 20 x 480 pixels, with the pixel depth of 1 bit. Afterwards, we carried out a comparative information-theoretic analysis encompassing the entire iris code.

We conducted a comparative analysis of the same iris population with the aim to confirm our assumption from the previous analysis. Three biometric templates (iris code) were generated for each iris for parameter values $\lambda_n = \{12,18,24\}$.

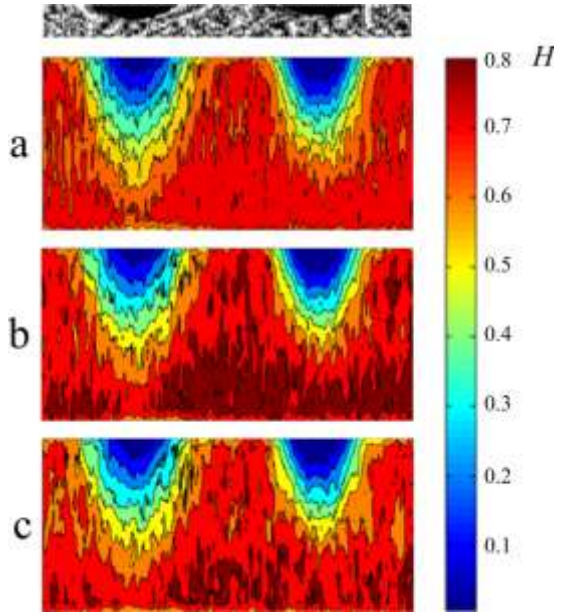

Figure 6
Iris coding transformation domain - varying the λ parameter a: λ = 12, b: λ = 18, c: λ = 24

As could be seen in Fig. 6 (a), the average information quantity or local entropy is equally distributed over the entire surface of iris code for parameter value λ = 12. This results in an average information quantity of 0.8412 per bit. Judging from the analysis of iris texture previously described, we cannot expect equal quality of information in both iris regions.

Fig. 6 (b) is the result of parameter value λ = 18. In the first region, we observe a characteristic information that is not equally present in the second region of the iris code. We obtain an average information quantity of 0.8189 per bit. This characteristic information corresponds to the results illustrated in Fig. 3.

The last measurement uses the value of λ = 24 and is depicted in Fig. 6. (c). The characteristic information is slowly vanishing from the first region, while it is almost nonexistent in the second region. This time, we obtain an average information quantity of 0.7982 per bit.

Varying the λ parameter is important for identifying the optimum filter values, which in turn produce stable and consistent bits with maximum entropy. Please note that by maximum entropy we actually refer to the best achieved compromise between maximum entropy and the largest number of consistent bits. Consistent bits comprise the characteristic information of the iris biometric source. This is of paramount importance for achieving a sound theoretical framework for development of BC systems. In our case, this compromise is arrived at for a filter bandwidth of λ = 18.

Table 1
Local entropy values by iris code regions

Window 9 x 9 / **Filter parameters**	**Region 1 - iris (bit per pixel)**	**Region 2 - iris (bit per pixel)**	**Regions 1 and 2 - iris (bit per pixel)**
λ = 12	0.9351	0.7251	0.8412
λ = 18	0.9125	0.6997	0.8189
λ = 24	0.8901	0.6776	0.7982

Table 1 presents summary results that clearly establish a significant difference between local entropy values of the first and the second region.

2.3 Analysis of Mutual Information between the Same and Different Irises

In this portion of information-theoretic analysis we use $\lambda = 18$ as the optimal filter bandwidth value in the iris coding transformation domain. By applying Shannon's approximation models [18], we determine the maximum entropy in the first region of the iris code. Adopting a method of approximation is crucial for properly estimating mutual information of identical and different irises.

The method as a whole is comprised of simple algorithms that were particularly developed for approximation models of orders II to V. We analyzed only the first iris code region. In the coding phase, we formed the matrix, row by row, based on the radial vectors in the normalization phase. The first row represents bits obtained through the first iris ring (radial vector). The rings are indicated in ascending order with the first being located closest to the pupil and the tenth farthest away from it since we only use the first iris region.

For instance, for an order II approximation, we assume a set of 4 possible messages, where messages are represented by numbers 1 to 4. For an order III approximation, we use numbers 1 to 8. Similar reasoning applies to higher order approximations. We assume that all messages have equal probabilities. For an order II approximation, iris code is decoded using a bigram. Fig. 7 provides an example of iris code decoding for an order II approximation by means of a dictionary. The process is similar for higher order approximations, with the number of words in the dictionary and the word length being increased.

Fig. 8 shows entropy levels for approximations of order II to V. Approximation V results in an entropy of 0.8208 per bit, which is the maximum value achieved by optimizing parameters in the transformation domain. Upon a closer look, entropy values for order V approximation are almost identical to local entropy for $\lambda = 18$.

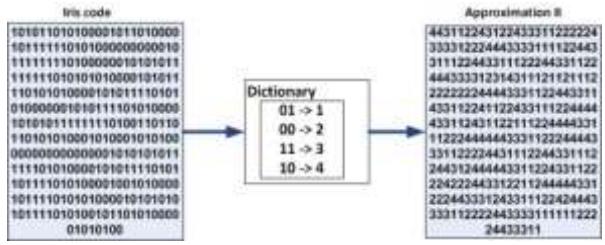

Figure 7
An example of order II approximation

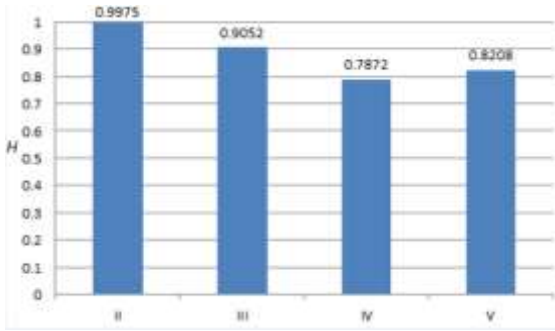

Figure 8
First iris region entropy for various approximation models (II - V)

Approximating for orders higher than V is possible, provided that all words in the dictionary exist. For this particular experiment (iris code) and order six approximation, many of the words in the dictionary had zero probability. This would not lead to a reliable entropy level. Hence, we restrict iris code to order V approximation. To that end, order V approximation is adopted for estimating mutual information. This approximation results in the entropy of 0.8208 per bit, which sums up to 3490 bits in the first iris code region.

2.4 Modeling of Iris Information Source using Shannon's Approximation Models

The following important analysis provides the calculation of mutual information between identical and different irises for the first region over the data obtained by order V approximation. The significance of this analysis is rather high concerning the security of BC systems. The method we use to measure mutual information I(iris x;iris y) between the two iris code regions is given by the following expression (2):

$$I(A,B) = \sum_{b\in B}\sum_{a\in A} p(a,b) * \log\left(\frac{p(a,b)}{p(a)p(b)}\right) \quad (2)$$

where:

- $p(a,b)$- joint probability distribution function of A and B
- $p(a)$ - marginal probability distribution function of A
- $p(b)$ - marginal probability distribution function of B

In the sense of probability theory, relative entropy of a system measures the distance between two probability distributions. In this way, mutual information is defined as (3):

$$\mathrm{I(A;B)} = \mathrm{H(A)} + \mathrm{H(B)} - \mathrm{H(A,B)}; \quad (3)$$

$$\mathrm{I(A;B)} = \mathrm{H(A)} - \mathrm{H(A|B)} = \mathrm{H(B)} - \mathrm{H(B|A)};$$

where:

- $H(A)$ – marginal entropy of A
- $H(B)$ – marginal entropy of B
- $H(A|B)$ – conditional entropy of A
- $H(B|A)$ – conditional entropy of B
- $H(A,B)$ – joint entropy of A and B

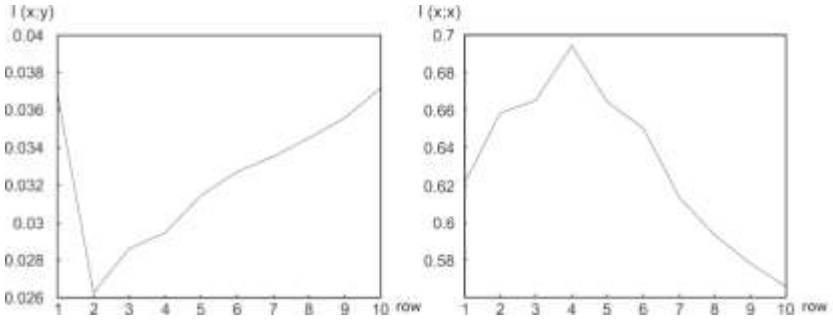

Figure 9

Mutual information between irises: left - different irises, right - the same irises

Fig. 9 illustrates the relationship of mutual information between the same and different irises by rows. Rows are shown on the x-axis. There are 10 rows in the first region and they are numbered in an ascending order, starting from the row closest to the pupil and ending farthest apart from it. Mutual information for two iris codes of a single person is $\mathrm{I(X;Y)} = 0.2078$ per bit or 997 bits totally. Please note that one always desires maximum mutual information between different images of the same iris.

In case of irises belonging to different people (Fig. 9 (a)), the average quantity of mutual information is $\mathrm{I(X;Y)} = 0.1065$ per bit or 511 bits totally. Such results guarantee the presence of consistent bits, in particular for the analysis of mutual information between the same rows. The interval between rows 3 and 6 contains

the maximum mutual information (same person irises), while the interval from the row 2 to row 6 (different people irises) measured minimum mutual information. We attribute this result to the algorithm parameters in the transformation domain.

2.5 Degrees of Freedom vs. Entropy

The complexity of iris code is approximately determined by measuring the Degrees of freedom (DOF, hereafter) over the corpus of different iris codes. DOF is calculated by means of all mutual Hamming distances as a binomial probability distribution.

DOF is also defined as a minimum number of independent coordinates that fully describe the state of a system. For the CASIA database, DOF is 1068, with 1D Gabor wavelet being used for coding of the source [21]. This is an exceptional result and guarantees the uniqueness and independence between different iris templates.

Table 2
Comparison of 1D and 2D wavelet demodulation

Iris template	Wavelet filters	DOF
2048 bits	2D Gabor	249
9600 bits	1D Gabor	1068

Table 2 compares the sizes of generated iris code and the DOF obtained between iris codes generated by 1D and 2D Gabor wavelets. When using a 1D Gabor wavelet, the generated iris code amounts to 9600 bits, whereas a 2D Gabor wavelet results in the iris code of 2048 bits [3].

Table 3
DOF after optimizing the wavelet filters

	Region 1 and 2 (9600 bits)	Region 1 (4800 bits)	Region 2 (4800 bits)
λ_n	DOF	DOF	DOF
12	2946.8	2217.5	935.5
18	1367.3	**1346.1**	396.7
24	654.5	785.0	199.3

Table 3 presents the DOF values by regions and for the iris code as a whole, obtained after the optimization of parameters in the transformation domain. We use three values of the λ_n parameter. For $\lambda_n = 18$ in the first iris region (size of 4800 bits) we measured DOF = 1346. This is a significant improvement compared to the data displayed in Table 2. Furthermore, the iris authentication features have not been compromised in any way.

2.6 Information-Theoretic Framework of Iris Biometrics

We begin by introducing the notation [12] needed to establish the information framework of iris biometry.

- $I(Y;Y')$ - mutual information between images of the same iris;
- $I(X;Y)$ - mutual information between images of different irises;
- $H(X)$ - entropy of iris code;
- $H(X,Y)$ - joint entropy of iris codes for two different eyes;
- $H(Y,Y')$ - entropy of two iris codes of the same person;
- $H(K)$ - joint entropy of two iris codes for the same eye;

Let us assume that the irises Y and Y' belong to Alice and are used in a certain BC system. On the other hand, iris X belongs to Eve, a potential attacker.

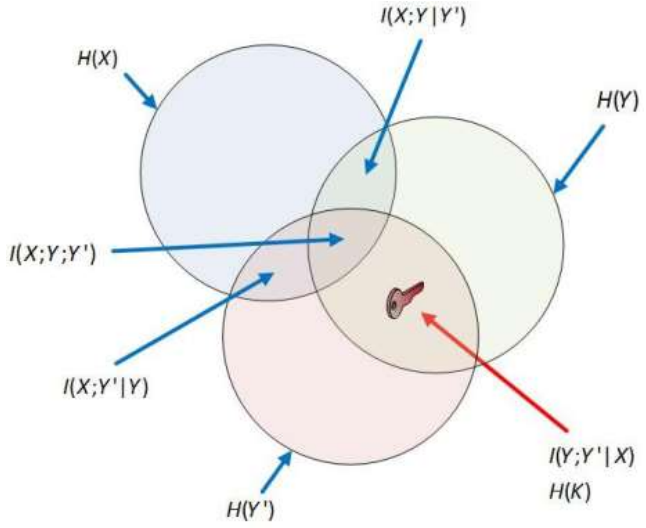

Figure 10

Graphic presentation of information-theoretic framework for development of BC systems

Fig. 10 illustrates an information-theoretic maximum for estimation of biometric keys used for development of BC systems. The diagram contains three random variables X, Y and Y'. It is important to note that the mutual information $I(X;Y;Y')$ is symmetric provided that the three variables are equally independent. A greater dependence between Y and Y', so is the mutual information $I(Y;Y')$ greater. This also entails that the information $I(Y;Y';X)$ is also greater. In this case, pairwise mutual information $I(X;Y)$ and $I(X;Y')$ have decreased, while the joint information $I(X;Y;Y')$ and $I(Y;Y'|X)$ have potentially increased.

Based on the analyses and measurements of entropy, we can numerically represent the quantity of information that is usable for creating an efficient BC system scheme. It is estimated that on average, the overall quantity of information present in the first region of an iris is $H(\text{iris } X) = H(\text{iris } Y) = H(\text{iris } Y') = 3940$ bits.

Mutual information between images of the same iris is $I(Y;Y') = 997$ bits, while mutual information between images of different irises is $I(X;Y) = 511$ bits. Joint entropy of two iris codes of two people is $H(X,Y) = 7281$ bits, whereas the joint entropy for images of the same iris is $H(Y,Y') = 6709$ bits. Also, we estimate that the overall quantity of useful information (i.e., entropy of the key) is $H(K) = I(Y;Y'|X) = 788$ bits, while the expected mutual information between all three variables (two same-person irises and another person's iris) is $I(X;Y;Y') = I(Y;Y') - I(Y,Y'|X) = 997 - 788 = 209$ bits.

2.7 Discussion

This work presents a method based on complex information-theoretic analysis of iris biometric that aims to extract homogeneous regions of high entropy. Successful extraction of these regions facilitates the development of effective systems for generation of cryptographic keys. Our method includes modeling of information sources – iris biometric. Shannon's model approximations, created real conditions for the application of information measures (entropy, mutual entropy, conditional entropy, joint entropy) to better understand the quality of the iris as biometric data. We also emphasized the importance of optimization wavelet parameters to achieve better results in the transformation domain. The results achieved in the work [11] prove this claim. At the same time, this approach allows for the application of simpler error correction codes with equal False Accept Rate levels, which reduces the overall complexity of this class of systems.

Conclusions

The main aim of this research was to enable the development of a professional class of systems for generation of long keys. We set out to meet the demands of modern cryptosystems relying on the existing components for coding biometric sources that encompass the entire process, starting from the choice of biometry, through imaging and ending with biometric templates.

The information-theoretic analysis used herein for the iris biometric data has confirmed our doubts. Moreover, it has led us to formulate clear goals in terms of raising the bar for system efficacy close to the theoretic maximum. In order to identify iris regions with the richest content of consistent information, we estimated entropy, local entropy, mutual information and employed Shannon approximations to model the information source. We performed parameter optimization of the appropriate wavelet transform with the aim to obtain the highest possible entropy and lowest possible information in the transformation domain.

Numerous authors have designed the schemes for systems that generate cryptographic keys based on the whole iris region. We demonstrated that the whole region cannot be used to develop such systems. The authors bypass the issues of low quality region and insufficient key length by increasing the capacity of error correction codes [11]. For this very reason, it is common among such systems to have FAR values above zero, which is unacceptable from our point of view. In addition, the keys generated in such manner rarely pass the common tests of cryptologic randomness (that include randomness and unpredictability).

Since the topic of this paper lies between biometrics and cryptography, we highlight the necessity of introducing the information-theoretic analysis in the increasingly popular field of biometric cryptography. This should be done with the aim of producing a firm bond between the two disciplines in a manner that is fully compliant with the cryptographic principles and characteristic features of biometric data.

We believe that the information-theoretic analysis employed in the course of development of this system guarantees high security performance needed for applications in law enforcement, military, government and diplomacy.

Acknowledgement

This work was supported by the Ministry of Science and Technological Development of the Republic of Serbia through the project TR32054.

References

[1] Matthieu Bloch, Joa o Barros: Physical-Layer Security: From Information Theory to Security Engineering (Cambridge University Press, 1st edn. 2011)

[2] F. Hao, R. Anderson, J. Daugman: Combining Crypto with Biometrics Effectively, IEEE Transactions on Computers, 2006, 55 (9) pp. 1081-1088

[3] J. Daugman: The Importance of Being Random, Statistical Principles of Iris Recognition, Pattern Recognition, 2003, 36 (2) pp. 279-291

[4] H. A. Garcia-Baleon, V. Alarcon-Aquino, O. Starostenko, et al.: Bimodal Biometric System for Cryptographic Key Generation Using Wavelet, Mexican International Conference on Computer Science- IEEE, 2009, pp. 186-196

[5] F. Hao and C. W. Chan.: Private Key Generation from On-Line Handwritten Signatures, Information Management & Computer Security, 2002, 10 (2) pp. 159-164

[6] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, et al.: Practical Biometric Authentication with Template Protection, AVBPA'05 Proceedings of the 5th international conference on Audio- and Video-Based Biometric Person Authentication, 2005, pp. 436-446

[7] M. van der Veen, T. Kevenaar, G.-J. Schrijen, et al.: Face Biometrics with Renewable Templates, Proc. SPIE 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII, 60720J, February 2006

[8] F. Monrose, M. K. Reiter, Q. Li, S. Wetzel.: Cryptographic Key Generation from Voice, In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001

[9] T. C. Clancy, N. Kiyavash, D. J. Lin.: Secure Smart Card-Based Fingerprint Authentication, Proc. ACM SIGMM Workshop Biometrics Methods and Application (WBMA), 2003

[10] J. Daugman: How Iris Recognition Works, Circuits and Systems for Video Technology. IEEE Transactions on, 2004, 14, pp. 21-30

[11] S. Adamovic, M. Milosavljevic, M. Veinovic, M. Sarac, A. Jevremovic: 'Fuzzy Commitment Scheme for Generation of Cryptographic Keys Based on Iris Biometrics', IET Biometrics, 2016, DOI: 10.1049/iet-bmt.2016.0061 IET Digital Library, http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2016.0061

[12] C. E. Shannon.: Communication Theory of Secrecy Systems, Bell System Technical Journal, 1949, 28, pp. 656-715

[13] S. Adamovic, M. Milosavljevic.: Information Analysis of Iris Biometrics for the Needs of Cryptology Key Extraction, Serbian Journal of Electrical Engineering, 2013, 10, 1, pp. 1-12

[14] 'Biometrics Ideal Test', http://biometrics.idealtest.org, accessed 15 October 2012

[15] T. Johar, P. Kaushik.: Iris Segmentation and Normalization using Daugman's Rubber Sheet Model, International Journal of Scientific and Technical Advancements, 2015, 1 (1) pp. 11-14

[16] S. Adamovic, A. G. Savic, M. Milosavljevic, et al.: Texture Analysis of Iris Biometrics based on Adaptive Size Neighborhood Entropy and Linear Discriminant Analysis, International Scientific Conference – Sinteza, Serbia, pp. 658-660, April 2014

[17] R. C. Gonzalez, R. E. Woods, S. L. Eddins: Digital Image Processing Using MATLAB, New Jersey, Prentice Hall, 2003

[18] C. E. Shannon.: A Mathematical Theory of Communication, Bell System Technical Journal, 1948, 27, pp. 379-423, 623-656

[19] T. Lee.: Image Representation using 2D Gabor Wavelets, IEEE Transactions of Pattern Analysis and Machine Intelligence, 1996, 18 (10) pp. 959-971

[20] Raymond W, Yueng.: A new Outlook on Shannon Information Measures, IEEE Transactions on IT., 1995, 37 (3) pp. 466-474

[21] L. Masek.: Recognition of Human Iris Patterns for Biometric Identification Iris Recognition, http://www.csse.uwa.edu.au/~pk/studentprojects/libor/., accessed 15 October 2012