SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 10, No. 1, February 2013, 1-12

UDK: 004.6.056.55 **DOI: 10.2298/SJEE1301001A**

Information Analysis of Iris Biometrics for the Needs of Cryptology Key Extraction

Saša Adamović[1], Milan Milosavljević[1,2]

Abstract: The paper presents a rigorous analysis of iris biometric information for the synthesis of an optimized system for the extraction of a high quality cryptology key. Estimations of local entropy and mutual information were identified as segments of the iris most suitable for this purpose. In order to optimize parameters, corresponding wavelets were transformed, in order to obtain the highest possible entropy and mutual information lower in the transformation domain, which set frameworks for the synthesis of systems for the extraction of truly random sequences of iris biometrics, without compromising authentication properties.

Keywords: Iris biometric, Mutual information, Entropy, Key extraction.

1 Introduction

Today's world of electronic communication creates a greater need for stronger access control to protect sensitive data. There is a great need for the introduction of modern and efficient methods of authentication against the best known forms of compromisation, being identity theft and impersonation. Traditional access control systems are based on the possession of passwords. Keys can be stored on smart cards, tokens or other devices for the same purposes. These devices cannot guarantee that users attempting to gain access to a service are legitimate.

Traditional cryptography uses a powerful mechanism to enhance information security. Current cryptographic algorithms (e.g., the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES)) have provable security status but their problem is the demanding length of the key distribution (64bit, 128bit, 256bit), the length being such that man lacks the ability to remember it. Research in the field of human identification still has many new challenges. For this reason, biometrics is imposed as a possible solution because of its vagueness and unique properties. Biometric systems are based on the physical or behavioral characteristics of human beings, such as face, voice,

[1]Singidunum University, Danijelova 32, 11000 Belgrade, Serbia; E-mail: sadamovic@singidunum.rs
[2]School of Electrical Engineering, Bulevar Kralja Aleksandra 73, 11000 Beograde, Serbia;
E-mail: mmilosavljevic@singidunum.ac.rs

fingerprint and iris. Biometric data has the potential advantage of becoming a unique identifier of a person. Depending on the type, the biometric samples may contain sufficient information that is hard to guess. To obtain the maximum amount of information from the iris, it is necessary to know the details of the extraction process and the different types of noise that affect the process of generating a biometric template.

The attractive features of the uniqueness of iris biometrics put then at the top of the biometrics list, but, on the other hand, they also have many weaknesses. Unlike passwords, lost or compromised biometrics cannot be reused or replaced with other biometric information. Based on these facts, we conclude that biometrics is a limited resource. Given the properties of biometric data, biometrics is becoming a serious candidate to replace the traditional password. The lack of a witness in iris biometrics is a complex way of processing [1], which significantly increases the variability of biometric data, and thus affects the quality of information in a biometric template. Problems of this type of system for the extraction of cryptology keys can be overcome by using appropriate techniques for signal processing and correction codes and fault detection.

Starting from theoretical foundations, and the concept of a perfect Shannon system, this paper will perform a rigorous analysis of iris biometrics necessary for the synthesis of optimized systems for the extraction of high quality cipher keys based on biometric data. A theoretical analysis of the information of iris biometrics as a kind of information source gives concrete solutions for the design of crypto-biometric systems with theoretically guaranteed performance.

The sections of the paper are as follows: Section 2 describes related work done by different scholars, Section 3 describes iris preprocessing and feature extraction, Section 4 describes the methods of analysis, Section 5 describes the results and Section 6 concludes.

2 Related Work

Authors F. Hao, R. Anderson and J. Daugman [2] have proposed an efficient method based on a combination of cryptographic and biometric data for the estimation of cryptographic keys. Their method does not require storage of reference data. The method is sensitive to errors, known as bursts of errors, which could affect the final system capacity. The main problem of their estimation method for the cryptographic key is that it uses a complete biometric iris template. Given the existence of a certain degree of correlation among irises, this is bad for the security parameters of this system.

Ali Shojaee Bakhtiari, Ali Asghar Beheshti Shirazi, and Amir Sepasi Zahmati [3] in his paper proposed using the iris segmentation method, based on analyzing the local entropy characteristic of the iris image, and the strengths and

weaknesses of the method are analyzed for practical purposes. Based on the propagation of local entropy, the segments are sorted based on the histogram segments for different purposes. In particular, the first ten segments with the highest entropy are allocated as estimation keys. The main problem of this method is that the final capacity of the system is not satisfactory.

Y.J. Chang, W. Zhang and T. Chen [4] introduced a method to map the extracted face features into bits, and a bit stream is used as the cryptographic key. A major problem with their method generation is that the biometric data is usually subject to drastic variation, and, in general, cannot produce exactly the same key.

K. Bae, S. Noh and J. Kim [5] proposed new feature extraction algorithm based on independent component analysis for iris recognition A conventional method based on Gabor wavelets should select parameters (e.g., spatial location, orientation, and frequency) for a fixed base.

3 Iris Preprocessing and Feature Extraction

In this section, we define two processes necessary for this analysis. Initially, preparing images for iris determination for local entropy and mutual information takes an 8-bit depth image. The first process is the process of localization and normalization. The final result is shown in Figs. 1 and 2. In the second process we apply the method to generate a biometric template of a normalized iris. The result is shown in Fig. 3.

3.1 Iris preprocessing

The first step requires the localization of the iris, insulating other regions of the human eye from digital photography. The process is very complex and crucial. If poorly positioned in a circle around the iris, the segmentation process will be unsuccessful, which is further reflected in poor authentication or increased FRR (*false rejection rate*) parameters, in our case cryptographic key reproducibility based on the obtained biometric information.

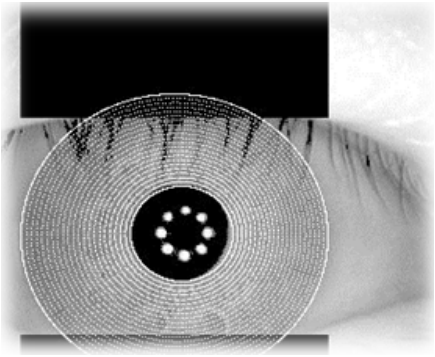

Fig. 1 – *Localized Iris.*

Fig. 1 shows the process of localization. The algorithm uses the Hough transformation [6]. The algorithm is used to determine the parameters of a geometric object, in this case a circle that describes the location of the iris. In addition to the localization algorithm, the performance of the segmentation process depends on the quality of the iris image.

Fig. 2 – *Normalized Iris.*

Fig. 2 shows the normalized iris localization process, the results of which we are directly used as templates in calculating the local entropy. The radial parameter for normalization is 20 pixels and the angle parameter for normalization is 240 pixels. The total normalized iris resolution is 240 x 20 pixels.

3.2 Iris feature extraction

In order to extract the discriminating features from the normalized iris region, the normalized pattern is convolved with 1-D Log-Gabor wavelets [7], equation (1). First, the 2-D normalized pattern is isolated into a number of 1-D signals, and then these 1-D signals are convolved with 1-D Gabor wavelets. The phase-quantization is applied to four levels on the outcomes of filtering with each filter producing two bits of data for each phasor. The total number of bits in the template will be the angular resolution times the radial resolution, times 2, times the number of filters used. The number of filters, their center frequencies and parameters of the modulating Gaussian function in order to achieve the best recognition rate and high entropy of biometric template.

$$G(f) = \exp\left(-\log\left(\frac{f}{f_0} \right)^2 \Big/ 2\left(\log\left(\frac{\sigma}{f_0} \right)^2 \right)^2 \right). \tag{1}$$

The optimum center wavelength for the CASIA dataset provided high local entropy when encoded using a filter with center wavelength of 12.0 pixels. Filter bandwidth with σ/f of 0.5, and template resolution of 20 pixels by 240 pixels was found to provide optimum encoding.

Fig. 3 shows the biometric template obtained after applying 1-D Gabor wavelets in the iris feature extraction process. The biometric template size is 9600 bits.

Fig. 3 – *Biometric template.*

4 Proposed Methods

4.1 Definition of local entropy method

According to Shannon's 2nd theorem [8] if the event *i* occurs from a set of valid events, with the probability *pi* the amount of uncertainty related to the event is equal to:

$$H_i = -\log_2\left(p_i\right). \tag{2}$$

Also the amount of uncertainty that the source of the events generates is equal to:

$$H_i = -\sum\left(p_i \log_2\left(p_i\right)\right). \tag{3}$$

The obtained result H_i, represents scalar value entropy of the grayscale (8-bit depth) images and can be used to characterize the texture of the iris image [9]. The value of p is a histogram which contains a series of frequencies depending on the aspect ratio. The standard for a grayscale picture has two logical outcomes of one or zero, a grayscale image has a value from 0 to 255 per pixel.

From equation (3) it can be seen that the highest amount of uncertainty from an information source is realized when the output symbols of the source are equally probable. The local entropy method divides the processed image into separate regions and then analyzes each region separately as an information source.

In this paper, we use the method for calculating the local entropy based on the selected window size. The number of windows is equal to the total number of pixels in the image. Each pixel is the center of a window by which we determine the entropy of each pixel. The designed method allows us to change the window size. The window is square (3×3, 5×5, ...) depending on the pixel resolution of the image. In the end we cannot precisely define the extent of the local information based on entropy in a two-dimensional iris image (Fig. 2).

Fig. 4 shows the process of determining the local entropy for the window size to 3×3 grayscale (8-bit depth) picture. The method for calculating the local entropy is defined as follows:

$$H_l[r_1, r_2, \ldots, r_i] = \text{entropy}(\text{image of iris}, \text{window size}).$$

The method returns an array H_i, where each pixel is determined by the entropy for a given window-size iris image. If the image has more than two dimensions, the method treats the image as a multi-dimensional picture. If calculating the local entropy of the image, it is necessary to provide a symmetrical complement of pixels which reflect the symmetric pixels with identical values of entropy.

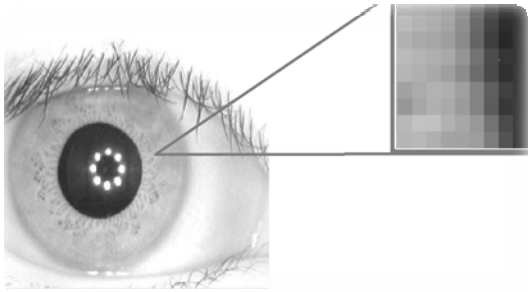

Fig. 4 – *Local entropy*.

4.2 Definition of mutual information

In addition to methods for determining the local entropy, we consider that the method for computing mutual information has an important role.

Size $I(X,Y)$ is called the mutual information between random variables X and Y. It is one of the central concepts of information theory. Strictly speaking it is not information, but the expected value of the amount of information we obtain from X when we observe the value of Y. This case corresponds to a fuzzy vault scheme. In general, the security of the fuzzy vault scheme depends on the mutual information of two different irises.

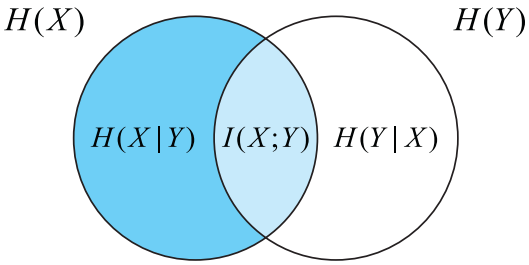

Fig. 5 – *Mutual information.*

Fig. 5 shows the graphical presentation of information-theoretic measures [8] for which the following statement is true:

$$I(X;Y) = H(X) - H(X|Y). \tag{4}$$

On the basis of (4), for this work, we calculated the mutual information of different and identical irises. The results of this experiment are shown in Section 5.

In paper [2], iris codes from the same eye usually disagree in 10 – 20% of the bits. On the other hand, the disagreement of interpersonal iris codes or the

codes for different eyes from the same person is usually 40 – 60%. We conclude that mutual information is essential in designing the system for the process of estimating the cryptographic keys, because the maximum mutual information between any two irises corresponds to a volume of information on the cryptographic key showing that the other person is known.

5 Results and Discussion

5.1 Iris datasets and development tool

The development tool used will be MATLAB®, and emphasis will only be on the software for performing recognition, and not the hardware for capturing an eye image[10]. A rapid application development approach will be employed in order to produce results quickly with an image processing toolbox, and high level programming methodology. To test the system, one data set of eye images will be used as inputs; CASIA-IrisV4 a database of 54,607 grayscale eye images courtesy of The Chinese Academy of Sciences – Institute of Automation (CASIA).

5.2 Local entropy

In the first part of the experiment, local entropy was calculated. Local entropy is determined by the level of the iris image. The resolution of the segmented iris is 240×20 pixels. The iris is divided into two regions. The first (1) is an inner region, which is positioned between the pupil and the outer region (2) iris. The outer region is positioned between the cornea and the inner region. The regions are clearly shown in Fig. 7.

The amount of information is expressed in bits per pixel, determined by the entropy of each pixel taken for the window size.

Table 1

The average values of local entropy in a sample of 70 *different irises.*

Region	3×3	5×5	7×7	9×9
1	2.6540	3.6379	4.1267	4.4412
2	2.1337	2.9149	3.3351	3.6020

Table 1 presents the results for four different dimensions of the window. Based on these results, we conclude that significantly higher local entropy is calculated in region 1. and found that the maximum entropy for the window size 9×9. The maximum value in the first region is 4.4412 bits per pixel and in the second 3.6020 bits per pixel. If the value of the entropy per pixel had a maximum value of 8 bits per pixel, the expected total amount of information per region would be 19,200 bits.

We showed that the total amount of information per pixel will vary significantly between regions. For this reason, we have made further comparisons which are given in Fig. 6. The values of local entropy in Fig. 6 represent the total amount of information in the regions to a certain level of window size. Values of local entropy are expressed in bits.

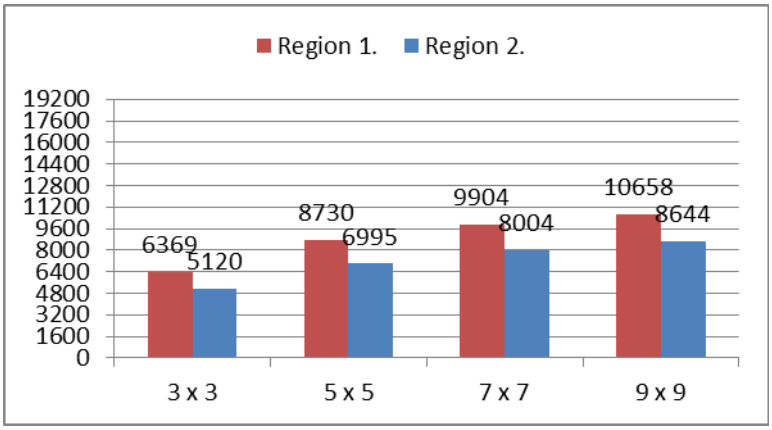

Fig. 6 – *The total amount of information by region.*

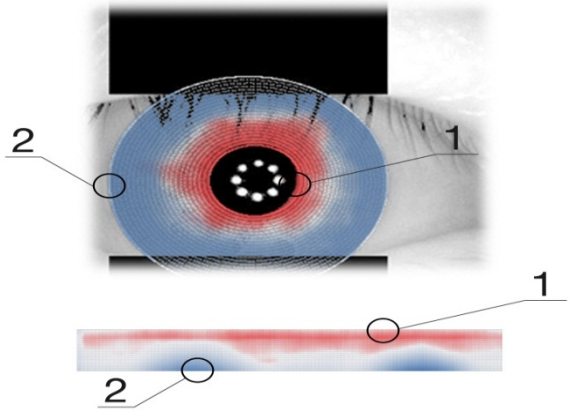

Fig. 7 – *Entropy of the iris texture by region.*

Fig. 7 clearly illustrates the extent of the value of the iris texture entropy and confirms a significant role of this method, described in Section 4. The iris texture, colored red, indicates increased entropy, and that colored blue indicates a significant decrease in the iris texture entropy.

In other measurements, local entropy is at the level of biometric iris templates. The resolution of the biometric template is 480×20 pixels. The template is treated as a black and white picture for which we calculated the local

entropy using the same method. In this experiment, we adopted a fixed value of a 9×9 window on the basis of the results obtained, and the image resolution. The biometric template generation process is described in Section 3. The iris is divided into two regions, identical to the previous experiment. The regions are clearly shown in Fig. 7

An important parameter in this part of the experiment is a parameter for determining the basis of the wavelength filter (W_l), the 1-D Gabor in the transformation domain. The ultimate goal was to determine the optimal value of this parameter. It was found that the optimal parameter value directly affects the entropy of the biometric template feature extraction process. This effect later positively affected the complete method of generating the cryptographic key. The values W_l in the wavelength of the filter basis were varied at 12, 18 and 24 pixels.

Table 2 shows the results for three values of the parameter of the wavelength filter basis (W_l). Based on these results, we concluded that the higher entropy calculated in first region of the iris. We found that the maximum entropy values were for the parameter value wavelength $W_l = 12$. The maximum value in the region of the first biometric template was 0.9582 bits per pixel, and the second region of 0.7482 bits per pixel. If the value of the entropy per pixel had a maximum value of 1 bit, the expected total amount of information per region would be 4,800 bits.

Table 2

The average values of local entropy in a sample of 70 *different irises.*

Region/ Wavelength	12	18	24
1.	0.9582	0.9536	0.9132
2.	0.7482	0.7228	0.7007

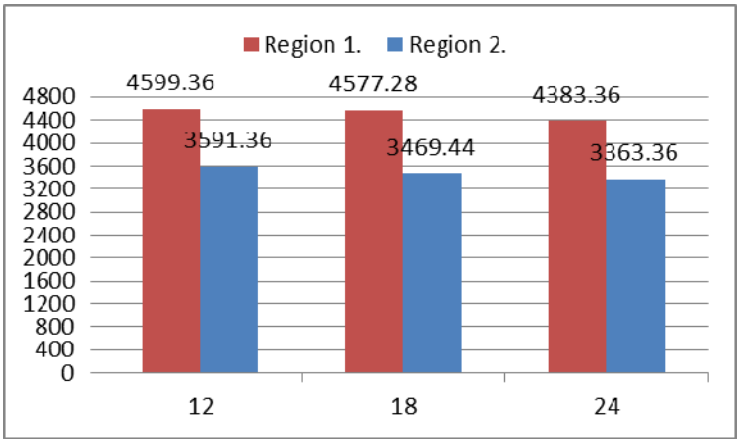

Fig. 8 – *The total amount of information by region.*

In **Table 2**, by varying the wavelength (W_l) parameter it may be noted that the total amount of information per pixel is significantly different. For this reason, we have made further comparisons which are given in Fig. 8. Values of the local entropy represent the total amount of information per parameter region for a certain level of wavelets. Values of the local entropy are expressed in bits.

5.3 Mutual information

In the third part of the experiment, the mutual information at the level of the iris biometric template is determined. The resolution of the biometric template is 480×20 pixels. The method of extracting a biometric template is described in Section 3. The biometric template we observed was the black and white image over which we applied the method described in Section 4 for the calculation of mutual information. The iris is divided into two regions identical to those in the previous experiment. We used the same set of iris samples.

In a previous experiment, we adopted the optimal parameter wavelength of the filter basis (W_l) for maximum uncertainty of the iris biometric templates. High uncertainty is very important for the safety of the estimation. The purpose of this method is to determine the maximum mutual information between the different regions of the same by the iris. The region that has the least mutual information among different irises is suitable for the synthesis of extracting cipher keys. On the other hand, regions that have been found to have maximum mutual information with identical irises are suitable for raising the performance of the algorithms for authentication.

Table 3 shows the results obtained after computing the mutual information on a sample of 70 different and 70 identical irises. The best result was obtained with the wavelength of the filter basis $W_l = 12$ which had the maximum mutual information of 0.0011 bits per pixel. With repeated experiments on the same iris, it was found that the first region has the largest mutual information, which is 0.0966 bits per pixel.

Table 3
Mutual information in different and same irises.

W_l	12	18	24
Region	Mutual information for different irises		
1.	0.0011	0.0015	0.0022
2.	0.0137	0.0163	0.0202
	Mutual information for identical irises		
1.	0.0966		
2.	0.0716		

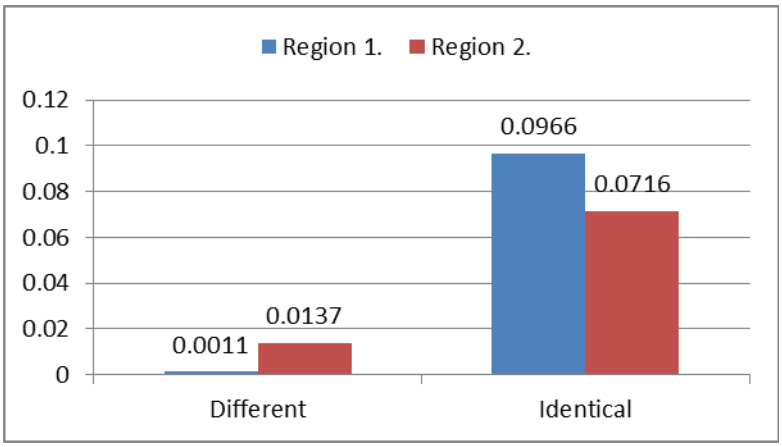

Fig. 9 – *The total amount of mutual information by region.*

The results show that the mutual information per pixel will vary significantly by region. For this reason, we made further comparisons which are given in Fig. 9. Values represent the amount of mutual information between the regions and various identical irises. The amount of mutual information by region is very important for the synthesis of systems for extracting cryptographic keys. On the other hand, this result confirms that the iris, as an information source, has ergodic properties. However, there are some indications that irises can be considered to be stationary ergodic sources.

6 Conclusion

Based on iris biometrics and with estimation of local entropy and mutual information, iris regions that are most suitable for generating cryptographic keys have been identified. In order to obtain the highest possible entropy and lower the mutual information in the transformation domain, the framework for the synthesis systems for estimating truly random bits from iris biometrics should be set, without compromising its existing authentication properties. Due to the variability of entropy in different regions and because of the correlation between any two different irises, we believe it is not safe to use the entire iris biometric template as estimation keys. It was found that, in parts of the iris, a decrease in entropy increases the mutual information.

Another interesting finding was that the encoding process only required one 1-D Log-Gabor filter to provide high entropy, since the open literature mentions the use of multiscale representation in the encoding process. Also, the optimum wavelength filter basis (W_l) was found to be important in the encoding process.

7 Acknowledgment

This work was supported by projects TR32054, III44006 financed by The Serbian Ministry of Education and Science.

8 References

[1] J. Daugman: How Iris Recognition Works, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, Jan. 2004, pp. 21 – 30.

[2] F. Hao, R. Anderson, J. Daugman: Combining Crypto with Biometrics Effectively, IEEE Transactions on Computers, Vol. 55, No. 9, Sept. 2006, pp. 1081 – 1088.

[3] A.S. Bakhtiari, A.A.B. Shirazi, A.S. Zahmati: An Efficient Segmentation Method based on Local Entropy Characteristics of Iris Biometrics, World Academy of Science, Engineering and Technology, No. 4, 2007, pp. 64 – 68.

[4] Y.J. Chang, W. Zhang, T. Chen: Biometrics-based Cryptographic Key Generation, IEEE International Conference on Multimedia and Expo, Taipei, Taiwan, 27 – 30 June 2004, Vol. 3, pp. 2203 – 2206.

[5] K. Bae, S. Noh, J. Kim: Iris Feature Extraction using Independent Component Analysis, 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, 09 – 11 June 2003, pp. 838 – 844.

[6] D.J. Kerbyson, T.J. Atherton: Circle Detection using Hough Transform Filters, 5th International Conference on Image Processing and its Applications, Edinburgh, UK, 04 – 06 July 1995, pp. 370 – 374.

[7] C. Sanchez-Avila, R. Sanchez-Reillo: Two Different Approaches for Iris Recognition using Gabor Filters and Multiscale Zero-crossing Representation, Pattern Recognition, Vol. 38, No. 2, Feb. 2005, pp. 231 – 240.

[8] R.W. Yueng: A New Outlook on Shannon's Information Measures, IEEE Transactions on Information Theory, Vol. 37, No. 3, May 1991, pp. 466 – 474.

[9] P. Kovesi: MATLAB Functions for Computer Vision and Image Analysis. Available at: http://www.csse.uwa.edu.au/~pk/Research/MatlabFns/index.html.

[10] K.W. Bowyer, K. Hollingsworth, P.J. Flynn: Image Understanding for Iris Biometrics: A Survey, Computer Vision and Image Understanding, Vol. 110, No. 2, May 2008, pp. 281 – 307.