An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level

Saad Abuguba, Milan M. Milosavljević and Nemanja Maček

Faculty of Informatics and Computing, Computer Technologies Department
Singidunum University, The School of Electrical and Computer Engineering of Applied Studies, Belgrade, Serbia

Abstract
Biometrics, defined as automated recognition of individuals based on their behavioral and biological characteristics, is beginning to gain acceptance as a legitimate authentication method and a practicable option to traditional identification methods in several application areas. Biometric cryptosystems, designed to generate a cryptographic key from a biometric trait, incorporate high level of security provided by cryptography and non-repudiation provided by biometry, as well as eliminating the need for a user to remember long passwords or carry tokens. Unlike unimodal biometric systems that employ single feature, multimodal biometric cryptosystems generate keys from two or more individual modalities typically fused at feature level. Fusing feature sets related to different modalities prevents possible spoof attacks and provides the system with higher level of overall security. This paper present an efficient approach to secure cryptographic key generation from iris and face biometric traits. Features extracted from preprocessed face and iris images are fused at the feature level and the multimodal biometric template is constructed from the Gabor filter and Principal Component Analysis outputs. This template is used to generate strong 256-bit cryptographic key. Experiments were performed using iris and face images from CASIA and ORL databases and the efficiency of the proposed approach is confirmed.

Key words:
biometrics; cryptography; feature fusion; face; iris; key generation

1. Introduction

“Biometrics is the science of establishing the identity of an individual based on physical, chemical or behavioral attributes of the person” [1]. Due to distinctive nature of biometric traits and non-repudiation it offers, biometry is frequently used to enhance the overall security of the system it is implemented in [2], e.g. biometric authentication systems or biometric cryptosystems.

There are two types of biometric systems: unimodal and multimodal. Unimodal systems employ single biometric sample, such as face or fingerprint. Multimodal systems employ two or more modalities, such as face and fingerprint. Using two or more modalities increases recognition accuracy, strengthens the proof as data is acquired from different sources [3], reduces false rejection rates (FRR) and false acceptance rates (FAR). Multimodal biometric systems are based on information fusion that can be performed on several levels, typically at feature, match score or decision level. Decision level [4] and matching score level [5] are applicable only to authentication systems, as they still result in two or more feature vectors that represent the identity of the user. The feature level fusion is based on generating new feature vector that represent the identity of an individual on the basis of feature vectors extracted from different modalities [6]. As the fusion outcome is one vector, feature level fusion can be used both in biometric authentication systems and biometric cryptosystems. While decision and match score level fusion is reported in numerous studies, fusion at the feature level is relatively understudied problem [7].

In biometric cryptosystems cryptography provides high level of security while biometry provides non-repudiation. Biometric cryptosystems can be roughly categorized into two groups: key generation and key binding systems. Key generation systems produce cryptographic key from acquired biometric data [8]. Key binding systems bind randomly generated cryptographic key to the biometric template [9] and release it when the appropriate biometric template is presented to the system. Recently, a great deal of attention have been paid to developing approaches for cryptographic key generation from biometric features and authenticating users by combining multiple biometric modalities.

The system presented in this paper generates a stable 256bit key generated from iris and face biometric traits. Key is generated from the Gabor filter and principal component analysis outputs fused at the feature level. The efficiency of proposed approach is experimentally evaluated using CASIA and ORL biometric template databases.

2. Related Work

Hao, Anderson and Daugman [10] have presented a biometric based cryptographic key generation method utilizing the iris feature and two-layer error correction technique that merges Hadamard and Reed-Solomon codes, thus providing a secure way to incorporate the iris

Manuscript received June 5, 2015
Manuscript revised June 20, 2015

biometrics into cryptographic applications. They produced an error free 140 bit key with acceptable 0.47% FRR and 0% FAR rates. Bae, Noh and Kim [11] have presented a novel iris recognition feature extraction algorithm based on independent component analysis. The proposed method reduces the size of the iris code and feature extraction time and has a similar Equal Error Rate (ERR) to conventional Gabor wavelets based methods.

Chen and Chandran [12] have presented a technique that produces deterministic bit sequences from the output of a repetitive one way transform via entropy based feature extraction process coupled with Reed Solomon error correcting codes. According to authors, the technique was evaluated with 3D face data and was confirmed to be reliable in 128 bit key generation. Teoh, Ngo and Goh [13] proposed a two-stage technique to generate personalized cryptographic keys from the face biometric, which offers the inextricably link to its owner. According to authors, tokenised face-hashing is rigorously protective of the face data, with security comparable to cryptographic hashing of token and knowledge key-factor. Beng, Teoh and Koh [14] have presented a biometric key generation scheme based on a randomized biometric helper. The technique consists of a randomized feature discretization process that enables one to control the intra-class variations of biometric data to the minimal level, and a code redundancy construction, that reduces the errors. The randomized biometric helper proved that a biometric key was easy to be invalidated as soon as the key get conciliated. Wu, Liu, Yuan and Xiao [15] have developed face biometric cryptosystem that uses 128-dimensional PCA vector and Reed-Solomon error correction codes. Sashank Singhvi, Venkatachalam, Kannan and Palanisamy [16] developed a technique that exploits an entropy dependent feature extraction process coupled with Reed-Solomon error correction, resolving an issue resulting from different acquisition of the similar biometric samples.

Feature vector concatenation followed by feature reduction transform is common form of feature level fusion. Feature level fusion proposed by Son and Lee [17] employs multi-level 2-D Daubechies wavelet transform applied to iris and face images and subdivision of resulting images into a grid. Features are extracted as the mean and standard deviation for each region and concatenated into a joint feature vector. Direct linear discriminant analysis is further applied to reduce the dimensionality of the vector. Gan, Gao and Liu [18] used two-dimensional discrete cosine transform (2D-DCT) for face and iris feature compression and Kernel Fisher Discriminant Analysis as feature fusion. This method was further improved by Gan and Liu [19] by employing Discrete Wavelet Transform instead of 2D-DCT, while the same fusion technique is used. The approach proposed by Rattani and Tistarelli [20] computes features using the scale-invariant feature transform (SIFT) algorithm applied to face and iris images. For each source, the extracted SIFT features are selected via spatial sampling and concatenated into a single feature vector using serial fusion. According to authors, the fused approach outperforms any unimodal biometric approach. Majority of the research in face-iris feature fusion reported in the literature is related to biometric authentication and the applicability of feature level fusion of iris and face to biometric cryptosystems is still understudied problem.

3. Feature Extraction and Key Generation

Before fusion and key generation is performed, iris and face features are extracted from provided biometric traits. This study adopts two notable, convenient extraction methods reported in the literature: principal component analysis and 2-D real Gabor filter.

3.1 Iris Feature Extraction and Normalization

Common iris biometric systems are based on the Daugman's methods [21]: iris image is identified, the region is unwrapped into a normalized, rectangular image and variants of Gabor filters are applied to extract iris features. The outer radius of iris patterns and pupils are first localized with Hough transform that involves canny edge detector to generate an edge map. Hugh transform identifies positions of circles and ellipses [22]. Hough transform for outer iris and pupil boundaries and a set of n recovered edge points (x_i, y_i) is defined by:

$$H\left(x_c, y_c, r\right) = \sum_{i=1}^{n} h\left(x_i, y_i, x_c, y_c, r\right), \qquad (1)$$

$$h\left(x_i, y_i, x_c, y_c, r\right) = \begin{cases} 1, \left(x_i - x_c\right)^2 + \left(y_i - y_c\right)^2 - r^2 = 0 \\ 0, \left(x_i - x_c\right)^2 + \left(y_i - y_c\right)^2 - r^2 \neq 0 \end{cases} \qquad (2)$$

The circle (x_c, y_c, r) through each edge point (x_i, y_i) is defined as:

$$\left(x_i - x_c\right)^2 + \left(y_i - y_c\right)^2 = r^2 . \qquad (3)$$

The triplet that maximizes $H(x_c, y_c, r)$ is common to the greatest number of edge points and is a reasonable choice to represent the contour of interest [23]. Once iris image is localized, **as shown in Fig 1**., regions of interests are defined and it is transformed into fixed-size rectangular image.

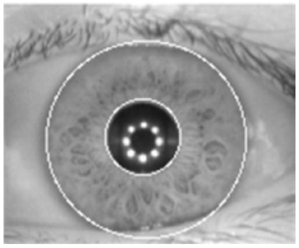

Fig. 1 Localized iris.

The normalization process employs Daugman's rubber sheet model that remaps the iris image $I(x, y)$ from Cartesian to polar coordinates [21], **as shown in Fig. 2**. Rubber sheet model produces a normalized representation with constant dimensions set by angular and radial resolution. If parameter r is on the interval [0, 1], θ is the angle [0, 2π], and iris and pupil boundary points along θ are denoted as (x_i, y_i) and (x_p, y_p), respectively, the transformation:

$$I\left(x\left(r,\theta\right), y\left(r,\theta\right)\right) \rightarrow I\left(r,\theta\right) \tag{4}$$

is performed according to:

$$x\left(r,\theta\right) = \left(1-r\right) x_p\left(\theta\right) + x_i\left(\theta\right), \tag{5}$$

$$y\left(r,\theta\right) = \left(1-r\right) y_p\left(\theta\right) + y_i\left(\theta\right). \tag{6}$$

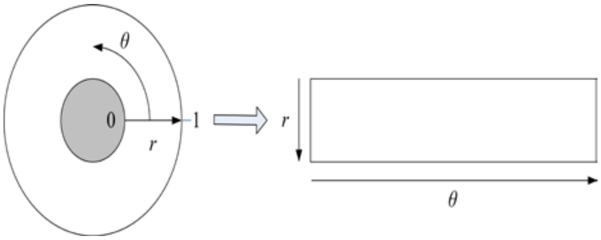

Fig. 2 Daugman’s rubbersheet model

Fig. 3 Normalized iris

Iris feature extraction is performed with 2-D real Gabor filters, as proposed by Wu, Qi, Wang and Zhang [24]. Let f denote the frequency of the sinusoidal plane wave, α and β are the space constants of the Gaussian envelope along x' and y' axis and θ the orientation of Gabor filter. Two-dimensional (2-D) real Gabor filter is given by:

$$G\left(x,y,\theta\right) = \frac{1}{2\pi\alpha\beta} e^{-\left(x'^2/2\alpha^2\right)-\left(y'^2/2\beta^2\right)} \cos\left(2\pi f x'\right), \tag{7}$$

$$x' = x\sin\theta + y\cos\theta, \tag{8}$$

$$y' = -x\cos\theta + y\sin\theta. \tag{9}$$

Four Gabor filters are applied with θ = 0, 45, 90 and 135 degrees, resulting in 4 filtered images. Details on Gabor filter parameters selection are discussed in [25]. Each filtered image is further divided in 16x4 rectangular 16 pixel wide blocks. Mean of each block is normalized to different range for the purpose of experimentation. Scaling to range [0,15] removes most of the noise originating from image distortion, while scaling to range [0,255] provides largest tolerance to brute force attacks. Iris 256-dimensional feature vector is constructed from 256 normalized means.

3.2 Face Feature Extraction

Face recognition is convenient, non-intrusive authentication method. There is various feature extraction methods from face biometrics reported in the literature. Roughly, they can be classified either as geometric or photometric approaches. Geometric approaches are based on developing the model based on geometric distances between fiducially points, while the photometric approaches are based on extracted statistical values [26].

Before the face features are extracted, input image is preprocessed. Preprocessing steps include image size normalization, background removal (region of interest selection), translation and rotational normalizations and illumination normalization. Normalization increases system robustness against posture, facial expression and illumination.

Principal component analysis (PCA) for face recognition is based on the information theory approach: it extracts relevant information and encodes it as efficiently as possible. PCA approach reveals the most effective low dimensional structure of facial patterns, removes information that is not useful and specifically decomposes the structure of face into uncorrelated components named Eigen faces [27]. Each image of face may be stored in a

1D array which is the representation of the weighted sum (feature vector) of the Eigen faces.

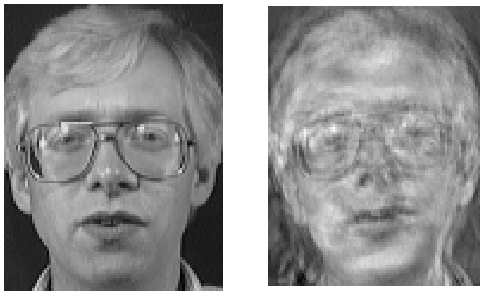

Fig. 4 Example image from ORL database and corresponding Eigenface.

This approach requires complete front view of face. According to [28], PCA can be summarized with the following steps. Let the face image X(*x*, *y*) be a two dimensional *m* x *n* array of intensities. The average face is defined by:

$$\overline{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \,, \tag{10}$$

where X_1, X_2, …. X_N denote training set images. The covariance matrix *C* given by:

$$C = \frac{1}{N}\sum_{i=1}^{N}\left(\overline{X} - X_i\right)\left(\overline{X} - X_i\right)^{\mathrm{T}} \tag{11}$$

represents the scatter degree of all feature vectors related to the average vector [29]. Let *V* denote the set of eigenvectors matrix *C* associated with its eigenvalue λ:

$$CV = \lambda V, V \in R_n, V \neq 0\,. \tag{12}$$

All training images of *i*-th person are projected to corresponding eigen-subspace, resulting in principal components, also known as eigenfaces:

$$y_k^i = w^{\mathrm{T}}\left(x_i\right), i = 1, \ldots N\,. \tag{13}$$

To reduce dimensionaliry, first N eigenvectors that have large variances are selected and remaining ones are discarded. Face data is further converted into local binary pattern that provides 256 bits of data.

3.3 Generating the Key from Face and Iris Features

Iris feature vector contains 256 normalized values, while the face provides 256 bits of useful data. Each bit of the 256-bit key is calculated by as follows:

- If the i-th bit of face local binary pattern is 0, then the *i*-th bit of the key is the sum all the zeros in binary representation of *i*-th normalized iris values modulus 2.
- If the i-th bit of face local binary pattern is 1, then the *i*-th bit of the key is the sum all the ones in binary representation of i-th normalized iris values modulus 2.

Resulting sums are concatenated and 256 bit key is generated.

4. Experimental Evaluation

The implementation of the proposed model is experimentally evaluated using MATLAB (version R2011b). Images from CASIA-IrisV4 [30], collected by the Chinese Academy of Sciences' Institute of Automation, and the well known ORL face database that is taken at the Olivetti Research Laboratory in Cambridge, UK [31] are used as inputs. Experiment fuses CASIA iris features with ORL face features. Because ORL face database includes 10 different images of each of 40 subjects, 40 iris images of CASIA database are selected to be fused with faces. Initial set of keys is generated for each fused subject during enrollment phase, and average false rejection rates are measured for different iris Gabor filter output normalization ranges. Experimental results are given in table 1

Table 1 Experimental Results

Normalization Range	***False Rejection Rates (%)***
[0, 15]	2.65 %
[0, 31]	3.08 %
[0, 63]	7.12 %
[0, 127]	9.59 %
[0, 255]	12.51 %

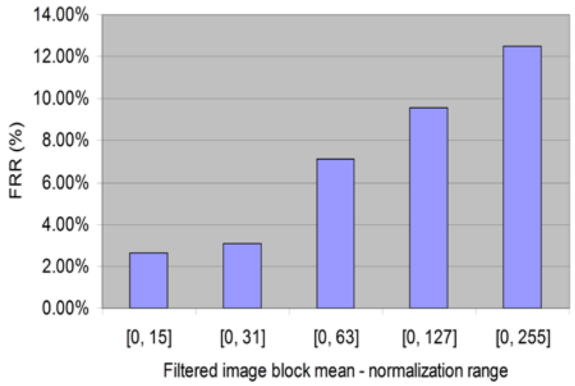

Fig. 5 Dependency of False Rejection Rate from filtered image block mean normalization range

5. Conclusions

This paper presents an efficient approach to cryptographic key generation from multiple biometric modalities. The system presented in this paper generates 256-bit crypto key generated from iris and face biometric traits. The proposed system employs three modules: feature extraction module, face feature extraction module and key generation module. The experiments performed with face images obtained from publicly available ORL database the iris images from CASIA-IrisV4 database have demonstrated the efficiency of the proposed approach to produce user-specific keys. Our further research will be focused on reducing the false rejection rates and implementing more advanced face feature extraction algorithms based on Normalized Principal Component Analysis and Gabor filters.

References

[1] A. K. Jain and A. Ross, “Introduction to Biometrics”, In “Handbook of Biometrics”, A. Jain et al. (Eds), Springer, 2008.

[2] P. Balakumar and R. Venkatesan, “A Survey on Biometrics based Cryptographic Key Generation Schemes”, International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012.

[3] L. Hong, A. K. Jain and S. Pankanti, “Can multibiometrics improve performance?”, In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, pp. 59-64, NJ, USA, 1999.

[4] S. Prabhakar and A. Jain, “Decision-level fusion in fingerprint verification. Pattern Recognition”, vol. 35, pp. 861-874, 2002.

[5] K. Toh, J. Kim and S. Lee, “Biometric scores fusion based on total error rate minimization”, Pattern Recognition, vol. 41, pp. 1066-1082, 2008.

[6] A. Ross and R. Govindarajan, “Feature Level Fusion in Biometric Systems”, In proceedings of Biometric Consortium Conference, September 2004.

[7] A. Ross and R. Govindarajan, “Feature level fusion of hand and face biometrics”. In Defense and Security (pp. 196-204). International Society for Optics and Photonics, 2005.

[8] Y. J. Chang, W. Zhang and T. Chen, “Biometrics-based cryptographic key generation”, In Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on (Vol. 3, pp. 2203-2206). IEEE.

[9] A. Juels and M. Sudan, “A fuzzy vault scheme”, In Proc. IEEE Int. Symp. Information Theory, IEEE Press, p. 408, 2002.

[10] F. Hao, R. Anderson and J. Daugman, “Combining crypto with biometrics effectively”, IEEE Transactions on Computers, Vol. 55, pp. 1081-1088, 2006.

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

[12] B. Chen and V. Chandran, “Biometric based cryptographic key generation from faces”, Digital Image Computing Techniques and Applications, 9th Biennial Conference of the Australian Pattern Recognition Society on. IEEE, 2007.

[13] A. B. Teoh, D. C. Ngo and A. Goh, “Personalised cryptographic key generation based on FaceHashing”, Computers & Security, 23(7), pp. 606-614, 2004.

[14] A. Beng, J. Teoh and A. K. Toh, “Secure biometric-key generation with biometric helper”, In Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on (pp. 2145-2150). IEEE.

[15] L. Wu, X. Liu, S. Yuan and P. Xiao, “A novel key generation cryptosystem based on face features”, In Signal Processing (ICSP), 2010 IEEE 10th International Conference on, pp. 1675-1678. IEEE.

[16] R. Sashank Singhvi, S. P. Venkatachalam, P. M. Kannan and V. Palanisamy, “Cryptography key generation using biometrics”, International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), pp. 1-6, 2009.

[17] B. Son and Y. Lee, “Biometric authentication system using reduced joint feature vector of iris and face”, In Audio-and Video-Based Biometric Person Authentication (pp. 513-522). Springer Berlin Heidelberg, 2005.

[18] Y. Gan, J. H. Gao and J. F. Liu, “Research on Face and Iris feature recognition based on 2DDCT and Kernel Fisher Discriminant Analysis”, In Wavelet Analysis and Pattern Recognition, 2008. ICWAPR'08. International Conference on (Vol. 1, pp. 401-405). IEEE.

[19] J. Y. Gan and J. F. Liu, “Fusion and recognition of face and iris feature based on wavelet feature and KFDA”, In Wavelet Analysis and Pattern Recognition, 2009. ICWAPR 2009. International Conference on (pp. 47-50). IEEE.

[20] A. Rattani and M. Tistarelli, “Robust multi-modal and multi-unit feature level fusion of face and iris biometrics”, In Advances in Biometrics (pp. 960-969). Springer Berlin Heidelberg, 2009.

[21] J. Daugman, “How iris recognition works”. Circuits and Systems for Video Technology, IEEE Transactions on, 14(1), pp. 21-30, 2004.

[22] D. J. Kerbyson and T. J. Atherton, “Circle Detection using Hough Transform Filters”, Fifth International Conference on Image Processing and its Applications, Edinburgh, UK, 04 – 06 July 1995, pp. 370-374.

[23] R. P. Wildes, “Iris recognition: an emerging biometric technology”, Proceedings of the IEEE, 85(9), pp. 1348-1363, 1997.

[24] X. Wu, N. Qi, K. Wang and D. Zhang, “An iris cryptosystem for information security”, In Intelligent

Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on (pp. 1533-1536). IEEE.

[25] D. Clausi and M. Jernigan, "Designing Gabor filters for optimal texture separability, Pattern Recognition, vol.33, pp. 1835-1849, Jan. 2000.

[26] R. Rouhi, M. Amiri and B. Irannejad, "A Review on Feature Extraction Techniques in Face Recognition", Signal & Image Processing: An International Journal (SIPIJ) Vol.3, No.6, December 2012, pp 1-14.

[27] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces", In Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition, Maui, Hawaii, pp.586-591, 1991.

[28] A. K. Bansal and P. Chawla, "Performance Evaluation of Face Recognition using PCA and N-PCA", International Journal of Computer Applications (0975 – 8887) Vol 76– No.8, August 2013, pp. 14-20.

[29] J. Daugman, "Face and gesture recognition: Overview", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 19, No. 7, pp. 675-676,1997.

[30] Biometrics Ideal Test, http://biometrics.idealtest.org

[31] AT&T Laboratories Cambridge Database of faces, http://www.uk.research.att.com:pub/data/att_faces.zip.

Saad Abuguba was born on 1974. He received the B.S. degree in Computer Engineering from Engineering Academy Tajoura in 1998 and M.Sc. degree in Electrical Engineering from Budapest University of Technology and Economics in 2006. He now is doing PhD study program in Advanced Information Safety System, field of natural and mathematical science, informatics and computing at Singidunum University, Belgrade, Serbia. His scientific research areas include information security, cryptology and biometric cryptosystem.

Milan Milosavljević was born in 1952, Ub, Serbia. He earned BS, MS and PhD degree from School of Electrical Engineering, Belgrade University in 1976, 1979 and 1982, respectively. From 1982 to 2003 he was vice director of the Institute for Applied Mathematics and Electronics, Belgrade, responsible for all its scientific research projects. Under his leadership the Institute for Applied Mathematics and Electronics became the leading scientific institutions in the former Yugoslavia. Since 2003 he has been working as a full professor at School of Electrical Engineering, Department of Signals and Systems. He was also head of the master program Modern Information Technology and PhD program Advanced Information Security Systems at Singidunum University, Belgrade.

His areas of expertise are pattern recognition, artificial intelligence, digital signal processing, machine learning, discrete optimization, and cryptanalysis and information security. He has published over 400 scientific bibliographic references and mentored more than 30 doctoral dissertations.

Nemanja Maček graduated from University of Novi Sad in 2006 and his PhD from Singidunum University, Belgrade in 2013. He works as teacher on several courses at School of Electrical and Computer Engineering of applied studies, and as a security consultant and researcher. Intrusion detection and machine learning and pattern recognition applied to security. He published several textbooks as coauthor, of which some are used as official university textbooks as well as number of papers in magazines and scientific conferences.