MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA
ISSN 2029-2341 print / ISSN 2029-2252 online
2011 3(1): 5–9 doi: 10.3846/mla.2011.001
Vaizdų technologijos T 111
Image Technologies T 111
Elektronika ir elektrotechnika
Electronics and Electrical Engineering

PRIVACY PRESERVING IRIS BASED BIOMETRIC IDENTITY VERIFICATION

Przemyslaw Strzelczyk[1,2]
[1]*Warsaw University of Technology, Warsaw, Poland*
[2]*Research and Academic Computer Network, Warsaw, Poland*
E-mail: pstrzelc@ia.pw.edu.pl

Abstract. Iris biometrics is considered one of the most accurate and robust methods of identity verification. Individually unique iris features can be presented in a compact binary form easily compared with reference template to confirm identity. However, when templates or features are disclosed, iris biometrics is no longer suitable for verification. Therefore, there is a need to perform iris feature matching without revealing the features itself and reference template. The paper proposes an extension of the standard iris-based verification protocol that introduces features and a template locking mechanism, which guarantees that no sensitive information is exposed.

Keywords: biometrics, iris recognition, privacy preserving, authentication.

Introduction

Among biometric verification methods, iris recognition is considered one of the most accurate and robust. Iris features can be easily extracted from eye images and efficiently compared. However, if biometric reference template or a set of biometric features are disclosed, the whole biometric system becomes useless for an individual, because biometric information cannot be cancelled or revoked as passwords. Therefore, there is a need to perform iris features matching without revealing either biometric data acquired during the verification process or reference template from the database. This paper introduces a privacy preserving system for iris-based biometric identity verification. First, we propose a method in which iris biometric templates stored by the authenticator are locked with the keys known only to the data owner. In this scenario, even when the database is compromised, no private information is exposed. Second, we introduce a privacy preserving verification protocol based on secure multi-party computation techniques.

Iris Biometrics

The iris is a collared ring around the pupil. The structure of the iris is determined during the fetal development of the eye and remains unchanged. On the contrary, the colour of the iris can change as a result of variable pigmentation in tissues. The main role of the iris is to control the size of the pupil and adjust the amount of light entering through the pupil into the eye interior. It is surrounded by the sclera, a white area of tissues and blood vessels, and is covered by a transparent layer called cornea. The whole iris is visible only when the eyes are wide open, as eyelids and eyelashes usually occlude the lower and upper part of it (Fig. 1).

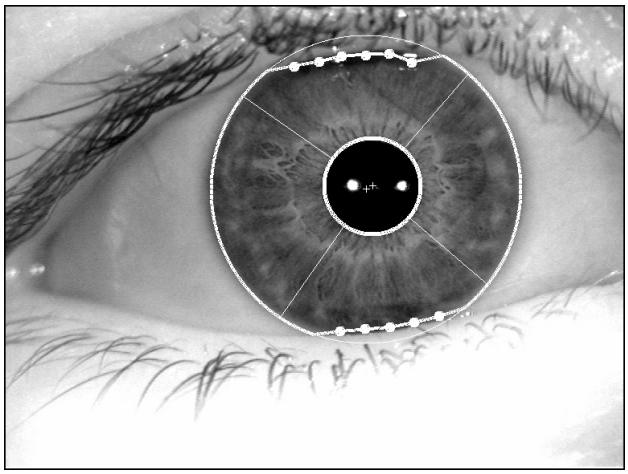

Fig. 1. An example of the eye image captured in infrared light with outer and inner boundaries approximated by non-concentric circles (*www.biometriclabs.pl*)

The possibility of using the iris to distinguish individuals is over 100 years old, but the first patent for the automated iris biometric system was obtained by Flom and Safir (1987). However, the most important work in the field of iris recognition was done by Daugman (1993, 1994). He introduced first practically verified methods for iris image segmentation and unique feature extraction and matching, which along with slight modifications are

presently used worldwide and which are the reference model for other algorithms.

For the purpose of biometrics, the eye image is captured in near infrared light with the wavelengths between 700–900 nm. Special infrared illuminators and bandpass lens filters are usually used for acquiring an image of a good quality. Infrared light reveals the detailed structure of the iris better than visible light (Daugman 2004). The iris is usually modelled as a ring with an outer and inner border approximated by two concentric unusual circles. Figure 1 shows an example image acquired in infrared light with the iris and pupil approximated by two circles. Because the iris area is hardly ever fully visible, an additional mask is applied to the ring, which marks the areas where eyelids and eyelashes occlude the iris region. Optionally, this mask also indicates image artifacts such as specular reflections from illuminators.

After the iris region is isolated, it is mapped into the normalized pseudo-polar coordinate system (Daugman 2004). Figure 2 shows the iris mapped into pseudo-polar coordinates.

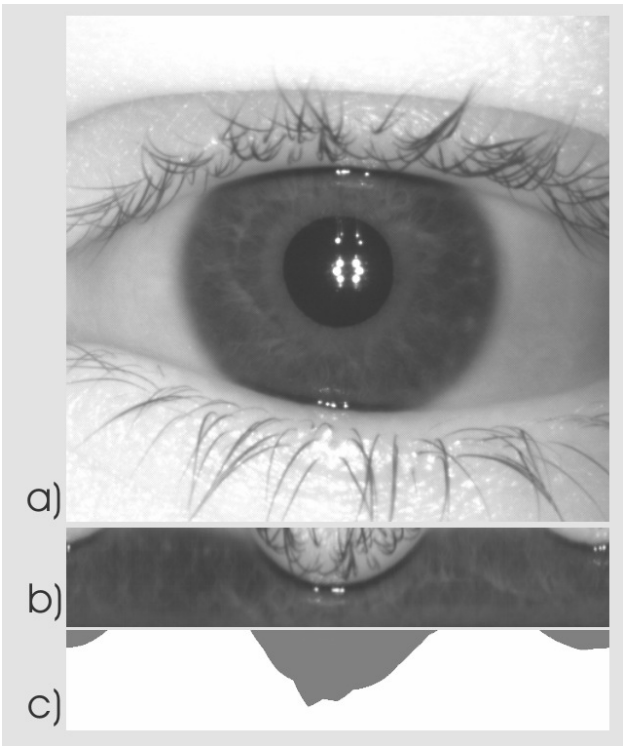

Fig. 2. An example of the iris image (a), the iris image converted to pseudo-polar coordinates (b) and occlusions mask in pseudo-polar coordinates

Every point of the iris area is described by two coordinates: angle α and radial distance r. When the pupil and the iris centre overlap, r is the normalized distance from the iris pupil centre, and α is the angle of the line crossing the point and the pupil centre.

The resulting rectangular image has two important properties. First, mapping models linear stretches of the iris when the pupil contracts or dilates, which is regarded a good approximation of its nature (Wyatt 2000). Second, the eye or head rotation is equivalent to the permutation of points in coordinate α, thus these effects can be easily compensated.

Most of iris biometric methods convolve the transformed image with 2-dimensional filters designed to extract unique iris texture patterns. Many different filters were tested but the best results were obtained for Gabor, Log-Gabor, Haar and Laplacian of Gaussian filters (Daugman 1994, 2004; Chenhong *et al.* 2005; Chou *et al.* 2006; Thornton *et al.* 2007; Yao *et al.* 2006). The resulting values are resampled and quantized. Daugman proposed that only the sign of the filtered signal should be used as features. He introduced a binary iris summarized in a vector of 2048 bits and called an 'iris code'. Many other solutions follow this approach as it allows the iris codes to be compared efficiently using bitwise operations (Daugman 1993).

Matching the iris code is based on the Hamming distance measuring the fraction of the corresponding bits of two disagreeing binary vectors. Considering the fact that not all of the bits of the iris code are valid due to occlusions and other disruptions, it should be taken into account that the modified Hamming distance must be introduced. It can be implemented using three types of operations, including bitwise XOR ($\oplus$), bitwise AND ($\wedge$) and bit counting and expressed as

$$HD(x, w, y, m) = \frac{\sum_i (x_i \oplus y_i) \wedge w_i \wedge m_i}{\sum_i w_i \wedge m_i}, \qquad (1)$$

where x and y are two iris codes and w and m are occlusions masks, the bits of which are set if the corresponding bits of the iris codes are valid. To account for eye rotation, the Hamming distance is computed for several different permutations of the bits corresponding to the different angles of rotations. At the end, the minimal score is compared with the predefined threshold to check if verification is successful.

Preserving Iris Code Privacy

Vernam's cryptographic system, known also as one-time pad is a type of the encryption method that has been proven to be impossible to crack if used properly (Shannon 1949). The main idea is that the plain text is encrypted with a substitution cipher using a secret random key. The size of the key must be equal to the size of the

plain text. As long as the key is truly random, and as large as the plain text, the resulting cipher text is also truly random.

For binary data, the Vernam's system of substitution can be implemented based on a cryptographically secure pseudorandom number generator and XOR operation. The pseudorandom number generator is used for preparing a key while XOR operation – for a random inversion of bit values based on the key bits. One-time pad is a symmetric encryption mechanism, as XOR operation when used twice with the same key reveals the original plain text.

The main idea behind privacy preserving iris based verification is that the iris codes encrypted with one-time pad can be matched in the same way as the unencrypted ones. The Hamming distance of two iris codes before and after encryption remain the same, as long as the keys used to encrypt them are identical. It is because XOR operation used for computing the Hamming distance nullifies encryption in the following way:

$$\mathrm{enc}_{\oplus}(x,k) \oplus \mathrm{enc}_{\oplus}(y,k) = x \oplus k \oplus y = x \oplus y \,. \qquad (2)$$

The biometric features of the same individual differ each time biometric measurements are done. For iris biometrics, this variability is mainly due to changing capture conditions and image processing. These processes introduce noise to the iris code. Whether noise is a user's characteristic or not is still an open question. Nevertheless, we can assume that for each individual an ideal iris code x' and specific noise measurement z exist. The real iris code can be expressed as XOR operation between ideal iris code x' and noise measurement z. In this situation, noise determines the Hamming distance between two iris codes of the same individual.

Now, if we use the same cryptographic key in one-time pad cipher for different real iris codes of the same individual, we may reveal information about noise but the ideal iris code remains encrypted. The iris code matching routine will not only nullify encryption but also the ideal iris code. An adversary will be able to determine the character of noise but will deduce nothing about the ideal iris code.

The presented encryption of the iris code has some other interesting features. The conducted experiments indicate that there is only about 100 to 200 bits of information in the iris code in the Shannon sense (Daugman 2005). This suggests that the bits of iris codes are strongly dependent. One-time pad encryption removes bit dependencies in cipher texts if the key used has its bits independent. As a result, the encrypted iris code will be indistinguishable from random data for an adversary.

Two-Party Protocol

The privacy preserving iris based biometric authentication protocol is based on the secure multi-party computation scheme and applies the one-time pad encryption of the iris code presented in the previous section. Two parties involved in this process will be later called Alice and Bob. Alice represents a user who is willing to undergo biometric verification. She does not want her biometric data (namely the iris code and binary occlusions mask) to be disclosed to any other party. Bob represents an authentication server verifying Alice identity based on her biometric data. Bob has access to the encrypted biometric templates database, which he does not want to disclose to anyone.

The authentication protocol presented in this paper employs several proven cryptographic methods. The first one is the cryptographic one-way function called a later hash function (Schneier 1996). It is a deterministic procedure which takes an arbitrary binary vector and transforms it into fixed size bit string, called a hash value. Transformation has some fundamental properties: it is easy to compute the hash, but it is infeasible to recover the binary vector from the hash value. It is infeasible to find two binary vectors with the same hash or modify the binary vector without changing its hash. A sample hash function suitable for our solution could be SHA-2.

The authentication scheme uses also a secure channel establishment technique (Schneier 1996). There are many algorithms that can be used for that purpose.

The protocol also requires a cryptographically secure pseudo-random number generator (CSPRNG) having a very long period, satisfying the 'next-bit test' and withstanding 'state compromise extensions' (Schneier 1996).

When Alice is enrolled into the biometric system, she uses a trusted biometric device capturing her iris images and generating her reference iris code with an optional occlusions mask. Then, the cryptographically secure pseudo-random number generator creates a secret encryption key used for encrypting the reference iris code. The hash value of the key is computed and the key is released to Alice. The hash code is needed in the verification process to prove that Bob poses the encrypted template of Alice. Bob does not have access to the encryption key. Instead, he receives the encrypted reference iris code with the associated mask and hash value of the

key. Bob inserts the hash value of the key and the encrypted template into his database indexed with identification numbers. Afterwards, the system is ready for biometric verification.

The verification process is described in Figure 3. When Alice wants to verify herself to Bob, she initializes a secure communication channel. Then, she generates random number q and sends it securely to Bob together with her claimed identity i. Bob uses random value q and the hash value of i-th key to prove Alice that her template is in the database. Additionally, he generates random number o which will be used by Alice to prove that she owns the proper key. Bob sends Alice number o and proof h^{**}. After the proof is checked by Alice, the biometric system captures her iris image and extract her iris code x occlusions associated with mask w. The iris code is encrypted with secret key k and proof h^{*} based on o is prepared. Encrypted iris code a^{*} with occlusion mask w and proof h^{*} are sent to Bob who verifies proof and calculates the Hamming distance between the encrypted iris code from Alice and the corresponding encrypted template from the database. If the Hamming distance is lower than the predefined threshold, verification is considered successful.

Conclusions

The presented methods allow authenticating an individual based on iris biometrics without revealing information about biometric features. These methods use the specific proprieties of the iris code and its matching routines, and employ proven and verified cryptographic techniques. The presented protocol can be incorporated into the existing authentication schemes. The author of this paper is working on the specification and reference implementation of the authentication server and client that will be used by the Extensible Authentication Protocol (EAP) family adapted to presented biometric requirements.

Our future work will focus on investigating the noise properties of the iris code. It is essential for the presented protocol to discover how much individual-specific information is still present in noise, and what can be done to make noise more random.

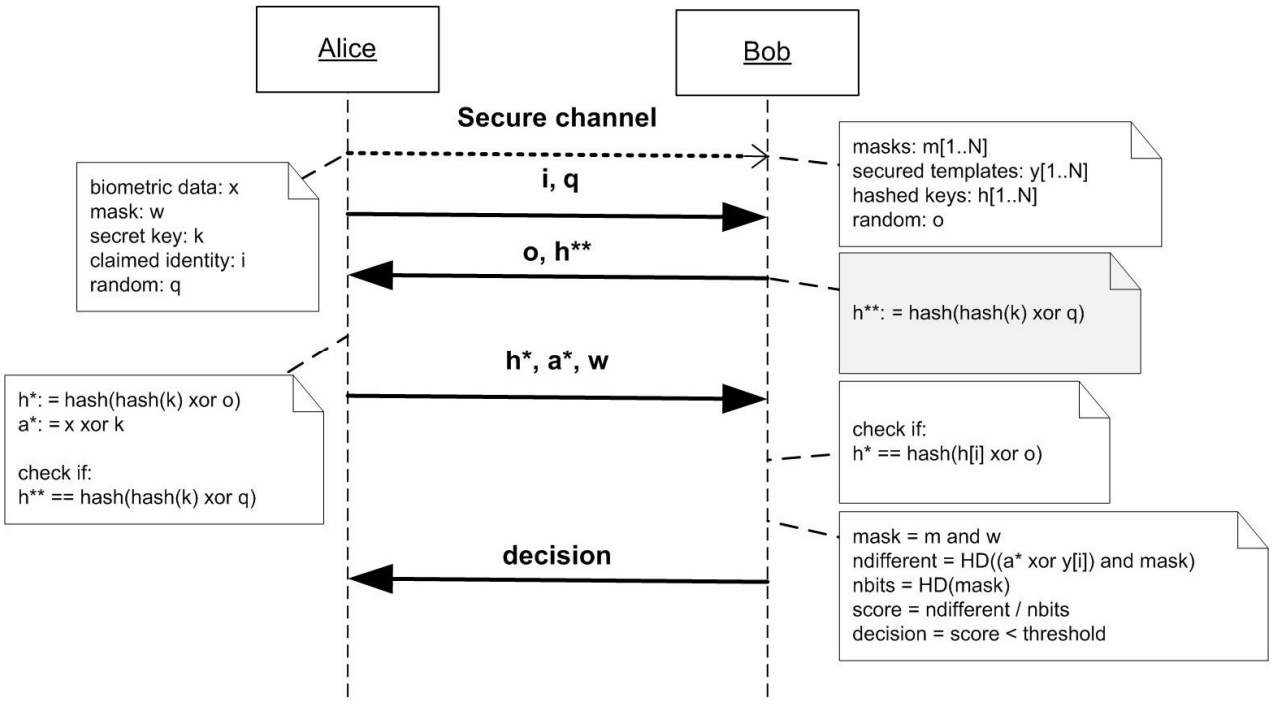

Fig. 3. A sequence diagram for the privacy preserving iris based biometric authentication protocol with two parties

References

Boles, W.; Boashash, B. 1998. A human identification techniques using images of the iris and wavelet transform, *IEEE Trans. Signal Process.* 46 (4): 1185–1188. doi:10.1109/78.668573

Chenhong, L.; Zhaoyang, L. 2005. Efficient iris recognition by computing discriminable textons, in *International Conference on Neural Networks and Brain*, 2: 1164–1167. doi:10.1109/ICNNB.2005.1614822

Chou, C.-T., *et al*. 2006. Iris recognition with multiscale edge-type matching, in *International Conference on Pattern Recognition*, 545–548.

Daugman, J. 1993. High confidence visual recognition of persons by test of statistical independence, *IEEE Trans. Pattern Anal. Mach. Intell.* 15(11): 1148–1161. doi:10.1109/34.244676

Daugman, J. 1994. *Biometric personal identification system based on iris analysis.* U.S. Patent No. 5,291,560.

Daugman, J. 2004. How iris recognition works, *IEEE Trans. Circ. Syst. Viedo Technol.* 14(1): 21–30. doi:10.1109/TCSVT.2003.818350

Daugman, J. 2005. *Results from 200 billion iris cross-comparisons*. Technical Report UCAM-CL-TR-635, University of Cambridge Computer Laboratory.

Flom, L.; Safir, A. 1987 *Iris recognition system.* U.S. Patent No. 3,641,349.

Schneier, B. 1996. *Applied Cryptography*. John Wiley & Sons. ISBN 0471128457.

Shannon, C. 1949. Communication Theory of Secrecy Systems, *Bell System Technical Journal* 28 (4): 656–715.

Thornton, J.; Savvides, M; Kumar, B.V.K. Vijava. 2007. An evaluation of iris pattern representations, in *Biometrics: Theory, Applications, and Systems*.

Wyatt, H. 2000. A minimum wear-and-tear meshwork for the iris, *Vis. Res*. 40: 2167–2176. doi:10.1016/S0042-6989(00)00068-7

Yao, P., *et al*. 2006. Iris recognition algorithm using modified Log-Gabor filters, in *International Conference on Pattern Recognition*, 461–464.

IŠSAUGANTIS PRIVATUMĄ, AKIES RAINELĖS ANALIZE GRĮSTAS, BIOMETRINIO TAPATUMO VERIFIKAVIMAS

P. Strzelczyk

Santrauka

Straipsnyje nagrinėjama biometrinio tapatumo, nustatomo pagal žmogaus akies rainelės vaizdą, verifikavimo problema. Pasiūlomas egzistuojančio standartinio biometrinio asmens tapatumo verifikavimo protokolo plėtinys, kuris remiasi rainelės požymių ir šablonų užraktais. Parodoma, kad šio patobulinto protokolo taikymas garantuoja privačios informacijos, išgaunamos iš asmens akies rainelės, slaptumą.

Reikšminiai žodžiai: biometrija, rainelės atpažinimas, privatumo išsaugojimas, autentifikavimas.