VNU Journal of Science, Natural Sciences and Technology 26 (2010) 14-20

Iris recognition for biometric passport authentication

Nguyen Ngoc Hoa*

Faculty of Information Technology, College of Technology, VNU, 144 Xuan Thuy, Hanoi, Vietnam

Received 29 October 2008

Abstract. This paper investigates an aspect of using iris recognition to authenticate a biometric passport. For this kind of authentication, two citizen's iris will be captured and stored on a RFID (Radio Frequency Identification) chip within two other biometrics: face and fingerprint. This chip is integrated into the cover of a passport, called a biometric passport. By using the iris recognition, a process of biometric passport authentication was presented in this paper by using the extended acces control, and allows integrate the verification result of the iris, face and fingerprint recognition. The integrating experiment will allow validate the accuracy of proprosal model in the near future.

Keywords: Biometric passport, extended access control, iris recognition, iris localization, iris extraction, iris matching.

1. Introduction

Iris recognition brings more advantages overs other biometric modalities as fingerprints, face,… It depends on the uniqueness of the human biometrics: iris. The later is a unique organ that is composed of pigmented vessels and ligaments forming unique linear marks, slight ridges, grooves, furrows, vasculature… [1]. Thus, comparing more features of iris allows to increase the likelihood of uniqueness. Another benefit of this biometric is its stability. The iris remains unchanged for a lifetime because it is not subjected to the environment, as it is protected by the cornea and aqueous humor. Therefore, many biometric researchers have used iris recognition for high confidence verification/identification and this has led to extensive studies in developing iris recognition techniques in unconstrained environments, where the probability of acquiring non-ideal iris images is very high due to off-angles, noise, blurring and occlusion by eyelashes, eyelids, glasses, and hair.

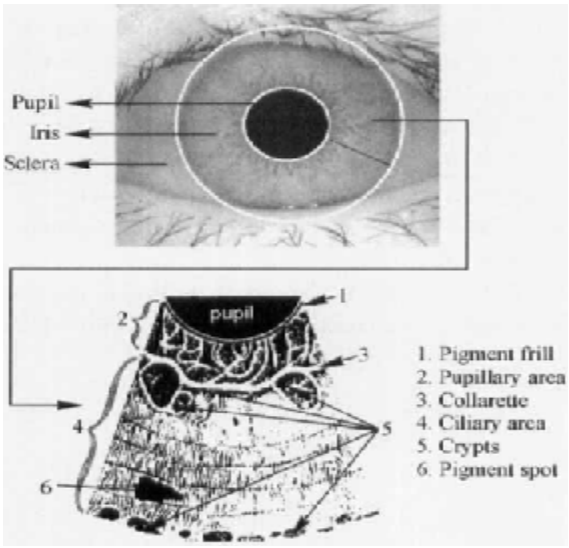

Fig. 1. Human iris.

* Tel.: 84-4-37547813.
E-mail: hoa.nguyen@vnu.edu.vn

The process of iris recognition is complex. It begins by scanning a person's iris by a special camera [2]. Then, by using a image processing technique, the iris will be located in the captured image following by another technique used to encodes the iris into a phase code (2048-bit) [3]. The phase code is then compared with a database of phase codes looking for a match. This step is normally very quick: more than 100,000 iris codes can be compared in a second executed in a normal computer [1].

In this paper, we concentrate to the view of using iris recognition in the way of applying this biometric for enhancing the process of biometric passport authentication. In the rest of this paper, we first introduce current approachs of iris recognition. The biometric passport concept will be detailed in the next section before the proposal integrating this biometric feature in the biometric passport authentication.

2. Iris recognition: state of the art

A typical iris recognition system commonly comprises six stages: iris image capture, iris segmentation, iris normalization, iris preprocessing (eyelids/eyelashes detection and iris image enhancement), feature extraction, and matching.

Many researchers have worked on various algorithms for iris recognition. Daugman [1,3] proposed a system based on phase code, using multi-scale Gabor wavelets for iris recognition and reported that it has excellent performance on a large database of many images. Wildes [4] described a method based on a pyramid of low-pass filtered images at different scales and then using the normalized correlation to find similarity of pixel intensities in the iris. Boles et al. [5] proposed an algorithm for extracting the iris features using zero crossing representation of 1-D wavelet transform. However, all these algorithms are based on grey images because of its important information enough to identify different individuals.

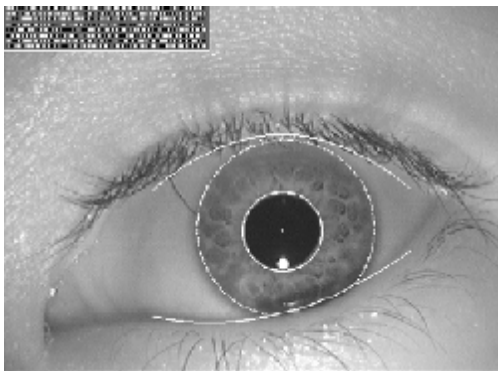

Fig.2. Example of iris pattern [3].

The iris identification/verification is basically divided in four steps: iris acquisition, localization, feature extraction and matching.

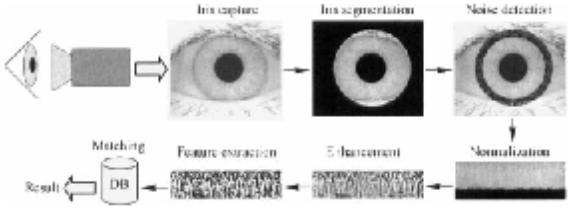

Fig.3. Stages of an iris recognition system.

2.1. Acquiring the iris

The iris acquirition is an important stage. Since iris is small in size and dark in color, it is difficult to acquire good image. Thus, it is normally captured by a special camera. The later will be used to take eye snaps while trying to maintain appropriate setting such as lighting, distance to the camera and resolution of the image. The camera needs to be able to photograph a picture in the 700 to 900 nanometers range so that it will not be detected by the person's iris during imaging [2]. The image is then changed from RGB to gray level for further processing.

In case of lack of the special camara for capturing the iris images, we can use the CASIA[1] iris image corpus available in the public domain for experiment. This corpus contains a total of 22,051 iris images from more than 700 subjects. All iris images are already 8 bit gray-level JPEG files, collected under near infrared illumination.

2.2. Locating the iris

Once the image of the iris is obtained, the iris needs to be located within the image. There are three variables within the image that are needed to fully locate the iris: the center coordinates, the iris radius, and the pupil radius [3]. An algorithm determines the maximum contour integral derivatives using the three variables to define a path of contour integration for each of the variables.The complex analysis of the algorithm finds the contour paths defining the outer and inner circumferences of the iris. Statistical estimation changes the circular paths of the integral derivatives toarc-shaped paths that best fit both iris boundaries.

Fig. 4 shows the overall procedure of the recent method for localizing the iris region within the eye image [6]. In this method, the inner and outer boundaries of the iris regions are detected by using two circular edge detection (CED) [7]. However, detection errors due to noise factors, such as occlusions of the eye due to eyeglasses and hair, are often observed. Therefore, the detected images are divided into two cases, namely ‘‘good-detection cases” and ‘‘bad-detection cases”, based on the existence of corneal specular reflection (SR). In the ‘‘good-detection cases”, the pupil and iris regions are correctly detected, and in the ‘‘bad-detection cases”, they are wrongly detected [6].

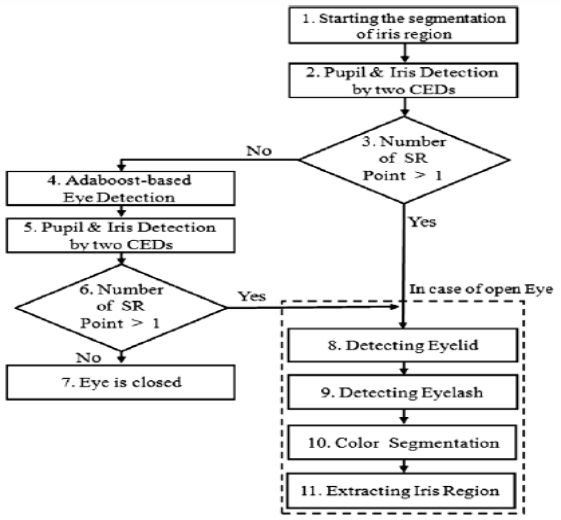

Fig.4. Iris locating process [6].

2.3. Extracting the iris features

Once the iris has been located, it must be encoded into an iris phase code. Daugman uses 2D Gabor filters to create more than two thousand phase bits from a raw image in a dimensionless polar coordinate system [1,3]. These kinds of filter used for iris recognition are defined in the doubly dimensionless polar Coordinate system(r,θ) as follow:

$$G(r,q) = e^{-iv\,(q-q_0)} e^{-(r-r_0)^2/a^2} e^{-i(q-q_0)^2/b^2}$$

Where r and θ specify the location of the function across the zones of analysis of iris. The α and β are the multiscale 2D wavelet size parameters. And ω is the wavelet frequency. Each isolated iris pattern is then demodulated to extract its phase information using quadrature 2D Gabor wavelets.

The disadvantage of the Gabor filter, not being band pass filters, lies on the fact that DC component whenever the bandwidth is larger than one octave [8]. However, the Log-Gabor filters are strictly band pass filters. So no DC

[1] See http://www.cbsr.ia.ac.cn/IrisDatabase.htm, for more detail information of CASIA iris image database - Institute of Automation Chinese Academy of Sciences.

components will pass the filters. [9] proposes convolving the normalized iris pattern with 2D Log-Gabor filters to generate iris code.

Another approach for features extraction was proposed by [10]. This method uses 2D Discrete Wavelet Transform (DWT) in order to extract the iris features. Results of using DWT for several kinds of wavelets: Haar, Daubechies, symlets… allow to validate the optimization of processing time and space.

2.3. Matching iris codes

Applying the matching algorithm on the input iris image and iris code existing in the database does the iris recognition. Normally, matching algorithm allows to determine the similarity between two given data sets. Thus, the iris image is said to be authentic if the result obtained after matching is more than the present threshold value.

Specifically, the number of iris code bits that need to correspond for a match must be determined [3]. The number of code bits required for a match is decided based on the specific application regarding how many irises need to be compared. The criteria used to decide if iris codes match is called the Hamming Distance (HD) criterion, which is the integration of the density function raised to the power of the number of independent tests.

Two similar irises will fail this test since distance between them will be small. The test of matching is implemented by the simple Boolean Exclusive-OR operator (XOR) applied to the 2048 bit phase vectors that encode any two iris patterns [3]. Letting A and B be two iris representations to be compared, this quantity can be calculated as with subscript ‘j’ indexing bit position and denoting the exclusive-OR operator.

$$HD = \frac{1}{2048}\sum_{i=1}^{2048} A_i \oplus B_i$$

A smaller criterion results in an exponentially decreasing chance of having a false match. This allows the strictness of matching irises to easily change for the particular application. A Hamming distance criterion of 0.26 gives the odds of a false match of 1 in 10 trillion, while a criterion of 0.32 gives the odds of 1 in 26 million.The numeric values of 0.26 and 0.32 represent the fractional amount that two iris codes can differ while still being considered a match in their respective instances [11].

3. Biometric passport

A biometric passport, or e-passport, is a combined paper and electronic identity document that uses biometrics to authenticate the identity of travelers. It uses contactless smart card (using the RFID[2] technology), including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or centre page, of the passport. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it virtually impossible to forge [12,13].

The currently standardized biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition. These were adopted after assessment of several different kinds of biometrics including retinal scan. The International Civil Aviation Organisation

[2] RFID: Radio Frequency IDentification

defines the biometric file formats and communication protocols to be used in passports. Only the digital image (usually in JPEG or JPEG2000 format) of each biometric feature is actually stored in the chip. The comparison of biometric features is performed outside the passport chip by electronic border control systems (e-borders). To store biometric data on the contactless chip, it includes a minimum of 32 kilobytes of EEPROM storage memory, and runs on an interface in accordance with the ISO/IEC 14443 international standard, amongst others. These standards ensure interoperability between different countries and different manufacturers of passport books [13].

4. Integration model

In our proposal, the biometric "iris" is used to enhance the quality of biometric passport authentication. By the standard of ICAO, the logical data structure of a biometric passport is organized by 16 data groups, numbered from DG1 to DG16 [14]. For using iris recognition, two iris images will be stored on the DG4, while two other biometrics, face and fingerprints, registered on the DG2 and DG3 respectively.

The process of biometric passport authentication is illustrated as the Fig.5. In case of having the Extended Access Control – EAC, we should verify two additional stages: authenticate the RFID chip on biometric passport, and authenticate the terminal (mutual authentication) [15, 16].

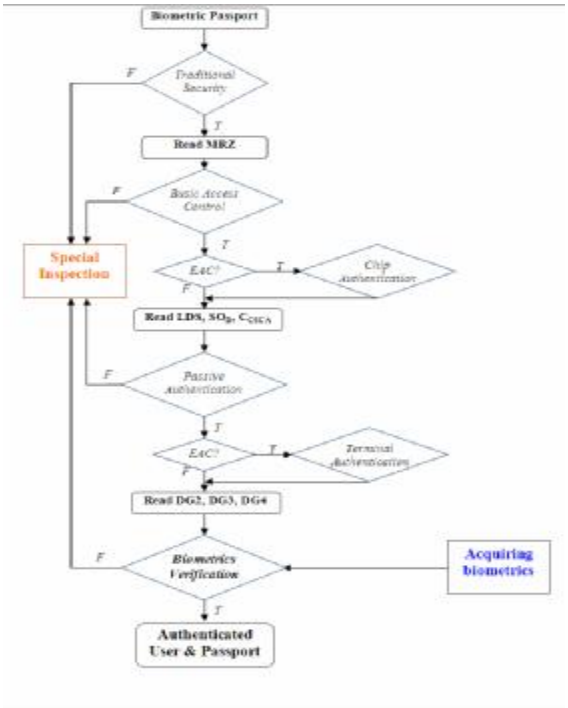

Fig.5 Process of biometric passport authentication.

In this paper, we concentrate mainly on the stage of verification of three biometrics: face, fingerprint and iris. Each biometric of a user will be captured from the dedicated device. Once we captured it, the inspection system should match it again the data stored on biometric passport.

For the iris recognition, the method of John Daugman is principally reused as the groundwork. The process of iris recognition is illustrated by the following steps:

- Locating the iris by using [6], obtained results are the iris region bounded by two "smart circles". This region will be segmented to a unwrapped image with the size of 480 x 40.

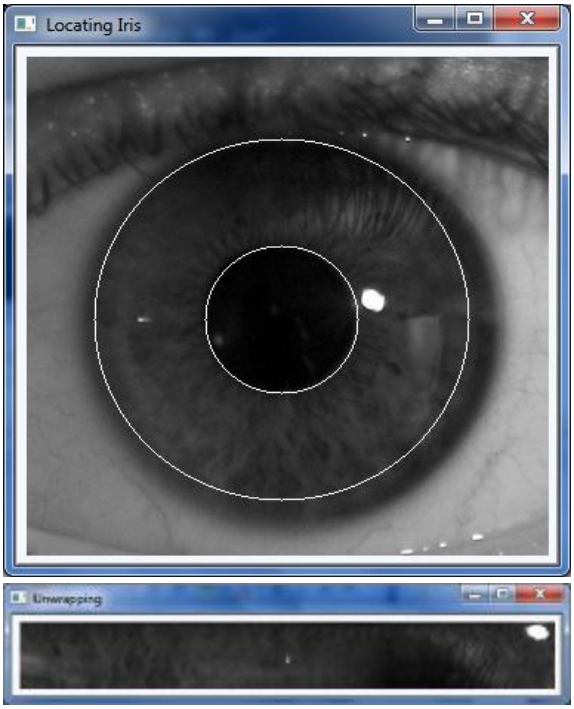

Fig.6. Locating an iris.

- Extracting the iris feature by using a Haar Wavelet that was described [10]. After using a Haar wavelet transform on the unwrapped images, along with some smoothing and normalization,we obtain an iris code (with size of 60 x 5 bytes)

Fig.7. Iris code extraction.

- The decision whether two iris codes match or differs is based on calculating their HD. A threshold is called Decision Value (DV) which was estimated in [11] at approx. 0.34 is used to take the decision.

The table below illustrates the execution time for difference steps of iris recognition. We tested 20 couple-irises for verifying by user's iris. The configuration of testing computer is Intel DualCore 2.0GHz, 1GB DDRRam.

Tab.1. Execution time for five steps in iris verification

Step	Time (milliseconds)
Locating pupil	16
Locating iris	1262
Unwrapping iris	15
Extracting iriscode	16
Verifying two iriscodes	249

This experiment validates the excellent possibility of using iris recognition for authenticating the biometric passport.

5. Conclusion

Iris recognition becomes now very useful and versatile security modality. It has proven to be a quick and accurate way of identifying an individual with no room for human error. Iris recognition is widely used in the transportation industry and can have many applications in other fields where security is necessary. Its use has been successful with little to no exception, and iris recognition will prove to be a widely used security measure in the future

Acknowledgments

This work is supported by the research projects N°. QC.08.04 and N° QG.09.28 granted by Vietnam National University, Hanoi, Vietnam.

References

[1] J.G. Daugman, The importance of being random: statistical principles of iris recognition, *IEEE Trans. Pattern Recogn.* 36 (2003) 279–291.

[2] Sean Henahan, The Eyes Have It. from *http://www.accessexecellence.org/WN/SU/irisscan.php*, retrieved May 26, 2009,

[3] J.G. Daugman, How iris recognition works, *IEEE Trans. Circ. Syst. Video Technol*. (2004) pp21–30.

[4] R. Wildes, "Iris recognition: an emerging biometric technology", *Proceedings of the IEEE, Vol. 85, No. 9*, September 1997.

[5] W. Boles, B. Bolash, "A human identification technique using images of the iris and wavelet transform", *IEEE transactions on signal processing, Vol. 46, issue 4*, pp1185-1188, 1998

[6] Dae Sik Jeong, Jae Won Hwang, Byung Jun Kang, Kang Ryoung Park, Chee Sun Won, Dong-Kwon Park, Jaihie Kim, A new iris segmentation method for non-ideal iris images, *Elsevier Journal of Image and Vision Computing*, In Press, Corrected Proof, 2009.

[7] D. Cho, K.R. Park, D.W. Rhee, Y. Kim, J. Yang, *Pupil and iris localization for iris recognition in mobile phones*, in: SNPD, Las Vegas, USA, June, 2006, pp19–20.

[8] D. Field, "*Relations between the statistics of natural images and the response properties of cortical cells*", J. Opt. Soc. Am.A/Vol: 4, 1987, pp. 2379 – 2394.

[9] Peng Yao et al, "*Iris Recognition Algorithm using modified Log Gabor Filters*", The 18th International Conference on Pattern Recognition(ICPR'06), IEEE Computer Society, 2006, pp. 461-464.

[10] F. Rossant, M. T. Eslava, T. Ea, F. Amiel and A. Amara, "Iris Identification and Robustness Evaluation of a Wavelet Packets Based Algorithm", *IEEE International Conference on Image Processing - ICIP '05*, Genova, September 11-14, 2005.

[11] Larsen, Richard J. & Marx, Morris L. *An Introduction to Mathematical Statistics and Its Application* (3rd ed.). Upper Saddle River, NJ: Prentice Hall. (2001).

[12] Juels, R. Pappu, S. Garfinkel, RFID Privacy: An Overview of Problems and Proposed Solutions, in *IEEE Security & Privacy*, vol. 3 (2005) 34.

[13] International Civil Aviation Organization, *Document 9303*, Part 1, Volumes 1 and 2, 6th edition, 2006.

[14] D.P Hanh et al, "Hộ chiếu điện tử và mô hình đề xuất tại Việt Nam", *Journal of Science & Technology of Vietnam National University at Hanoi*, (2007).

[15] D.T. Hien, et al., "Mutual Authentication for RFID tag-reader by using the elliptic curve cryptography", *Journal of Science & Technology of Vietnam National University at Hanoi*, (2008).

[16] P.T. Long, N.N. Hoa, "*Mô hình xác thực hộ chiếu điện tử*", tại Hội thảo Quốc gia "Một số vấn đề chọn lọc trong CNTT, Huế, Việt Nam (2008).

Ứng dụng nhận dạng mống mắt trong xác thực hộ chiếu sinh trắc

Nguyễn Ngọc Hóa

Khoa Công nghệ Thông tin, Trường Đại học Công nghệ, ĐHQGHN, 144 Xuân Thủy, Hà Nội, Việt Nam

Bài báo này giới thiệu mô hình ứng dụng kết quả của bài toán nhận dạng ảnh mống mắt trong việc xác thực người mang hộ chiếu sinh trắc. Là một trong những đặc trưng sinh trắc có độ chính xác rất cao trong việc xác thực người dùng (chỉ sau xác thực ADN), việc kết hợp nhận dạng mống mắt với hai đặc trưng sinh trắc phổ dụng khác là ảnh mặt người và ảnh vân tay sẽ cho phép nâng cao kết quả xác thực. Từ đó, quy trình xác thực người mang hộ chiếu sinh trắc sẽ được xây dựng dựa trên việc bổ sung phần kiểm soát truy cập mở rộng, cho phép tích hợp các kết quả nhận dạng mống mắt, ảnh mặt người và vân tay. Việc tích hợp sẽ được tiến hành trong thời gian tới và sẽ cho phép minh chứng rõ nét mô hình xác thực hộ chiếu tích hợp này.