INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

TECHNIKI INFORMACYJNE TEORIA I ZASTOSOWANIA

Wybrane problemy
Tom 2 (14)

poprzednio

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Pod redakcją
Andrzeja MYŚLIŃSKIEGO

Warszawa 2012

INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

TECHNIKI INFORMACYJNE TEORIA I ZASTOSOWANIA

Wybrane problemy
Tom 2 (14)

poprzednio

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Pod redakcją
Andrzeja Myślińskiego

Warszawa 2012

Wykaz opiniodawców artykułów zamieszczonych w niniejszym tomie:

Dr hab. inż. Andrzej MYŚLIŃSKI, prof. PAN

Dr hab. inż. Ryszard SMARZEWSKI, prof. KUL

Dr hab. Dominik ŚLĘZAK

Prof. dr hab. inż. Andrzej STRASZAK

Prof. dr hab. inż. Stanisław WALUKIEWICZ

Dr hab. Adam WIERZBICKI

ISBN 9788389475442

Biometric systems - concept and data acquisition of finger vein patterns

Piotr Fronc

Studia Doktoranckie IBS PAN,
e-mail: *piotr.fronc@pixie-labs.com*

Abstract.. In this paper, a brief description of biometric system concept is given, providing state-of-art commercial system implementations for financial sector. This is followed by a proposition of image acquisition device prototype created in order to obtain vascular pattern of a finger. Furthermore, a concept of biometric identification system using device prototype, along with feature extraction algorithm, is presented. Direction of future studies is given.

Key words: Vascular biometrics, biometric authentication, image acquisition

1 Biometric systems

1.1 Biometric system concept

The shortest definition of a biometric system would be that it is a system providing methods either to confirm an individual's identity or identify individual from given population operating on individual's external (eg. fingerprints) or internal (eg. vein patterns), direct (eg. hand shape) or indirect (eg. handwriting dynamics) features. Biometric system always operates on a set of previously obtained biometric data. This data set is a subject to pattern recognition algorithms. In other words, a biometric system is a specialized pattern recognition system which operates on a database of biometric templates created in a process of data acquisition followed by feature extraction. This process paired with pattern to person mapping is called enrollment and it must be prior to authentication or identification.

As mentioned above, there are two main groups of biometric systems: biometric authentication systems (verification of individual's identity) and biometric identification systems (identification of individual from limited population). These two classes, apart from area of implementation, differ in terms of two essential parameters that characterize biometric systems: False Match Rate (abr. FMR, also called False Positive) and False Non Match Rate (abr $FNMR$, also called False Negative).

Let the registered biometric template of person I be X_I. Let the acquired for verification biometric template of person Q be X_Q. According to Jain et al. [1], let the hypothesis H_0 be that template X_Q was obtained from a different person than template X_I and hypothesis H_1 be that template X_Q was obtained from the same individual as X_I. This implies the following verification decisions: D_0 - individual is an impostor and D_1 - verified individual. The FMR parameter is in fact a probability of making decision D_1 when hypothesis H_0 is true. The $FNMR$ parameter is a probability of making decision D_0 when hypothesis H_1 is true. Formulas (1) and (2) below are given after Jain et al.[1].

$$FMR = P(D_1|H_0) \tag{1}$$

$$FNMR = P(D_0|H_1) \tag{2}$$

While biometric authentication systems designers minimize the FMR parameter while allowing the $FNMR$ to be at a certain acceptable and relatively high level, biometric identification systems designers minimize the $FNMR$ parameter permitting FMR to be higher (a result of identification might be a set of several suboptimal matches).

Connected to FMR and $FNMR$ parameters are False Acceptance Rate (abr. FAR) and False Rejection Rate (abr. FRR) [3]:

$$FAR = FMR * (1 - FTA) \tag{3}$$

$$FRR = FTA + FNMR * (1 - FTA) \tag{4}$$

where: FTA - Failed To Acquire - rate of unsuccessful data acquisition processes.

Another, rather non-formal, classification is in terms of authentication (identification) process execution time. Some implementations, such as authentication in Automated Teller Machines (abr. ATM) require determining maximum time to establishing authentication decision, whereas other — eg. forensic systems — do not need such rigid time limitations.

1.2 Vascular biometrics

Vascular biometric systems operate on patterns of veins underneath human skin. There are several widely used regions of human body from which vein patterns can be obtained. These are hand palms, fingers and face. Vein patterns from these regions are recognized as unique, similarly to finger print patterns. In terms of unauthorized pattern usage, however, measured

by ability to obtain vein pattern without subject's knowledge and permission, finger vein and palm vein patterns seem to represent a vast improvement to system's security over finger printing methods.

Vein pattern is obtained by capturing image form CCD or CMOS sensor. Acquisition subject is first illuminated with infra-red or near infra-red light. Oxidized hemoglobin within subject's veins absorbs infra red radiation, thus veins in the image will appear as dark lines. Thanks to this effect, vascular methods have also, again, great security advantage over finger printing methods: "dead" tissue would not contain oxidized hemoglobin, therefore, veins would not be visible in acquired image, resulting a non-match decision.

Vein patterns of different fingers of the same person are not correlated, which means that every vein pattern of each finger can be treated as a template of distinct origin.

1.3 Commercial implementations for financial sector in Poland

Several banks from agricultural sector in Poland employ biometric authentication systems in their ATMs in cash withdrawal process. These implementations were first used in order to dispense social benefits to people who do not own their personal banking accounts, therefore no credit or debit cards were used as a form of identification token in favor of personal identification number (PESEL) or birth date. All of these implementations used Hitachi VeinID finger vein authentication technology, namely HOTS 602UE and 609UE devices. FAR and FRR parameter values for both of these devices are less than 0.0001% and 0.01% respectively, according to Japanese Industrial Standard JIS TR X0079 [3] .

Fig. 1. FingerVein enabled ATM.

The spoken biometric authentication system for financial operations authorization consist of three classes of components: server software, client software and biometric devices. Both HOTS device types used in banks perform template encryption and matching operations. Server software — apart from financial functions — manages biometric templates, device information, user privileges and template delivery. Client templates stored in a database are encrypted using hardware encryption keys which — at risk of potential security breach — does not allow attacker to obtain information on actual vein patterns. Also, communication between HOTS devices and controlling computer is encrypted. Server software also performs communication bus functions. Client software is essentially communication client for both ATM and user devices.

To the date, apart from social benefit payment, several other banks introduced biometric authentication system integrate with their central banking systems enabling their clients to withdraw money from personal accounts using biometric verification in ATMs.

2 Data acquisition device prototype

2.1 Device schematics

A custom data acquisition device is a key element of the system. Device consists of four main elements: CCD camera, two LED matrices, IR filter and frame grabber. Finger is illuminated by near infrared light emitted by LED matrices. IR filter lies below LED matrices. This element filters visible light leaving infrared range of spectrum to the camera. CCD sensor is situated below an IR filter and is connected to a frame grabber. Through frame grabber, image is transferred to the PC. Device schematics are presented in Fig. 2. Image of a prototype device is presented in Fig. 3.

2.2 Lighting subsystem

Lighting subsystem consists of two LED matrices. Each matrix consists of 5 LEDs organized in a row. Each LED emits near-infrared light of wave length $880nm$. Below, characteristics of oxidized hemoglobin and CCD sensor near infra-red absorption are given.

Wave length $880nm$ was chosen experimentally basing on absorption curves given in Fig. 4 and Fig. 5. For discussed wave length oxidized hemoglobin light absorption is near its local maximum for infra-red range while unoxidized hemoglobin light absorption is relatively low. Also, CCD sensor light absorption is still relatively high (above 40%).

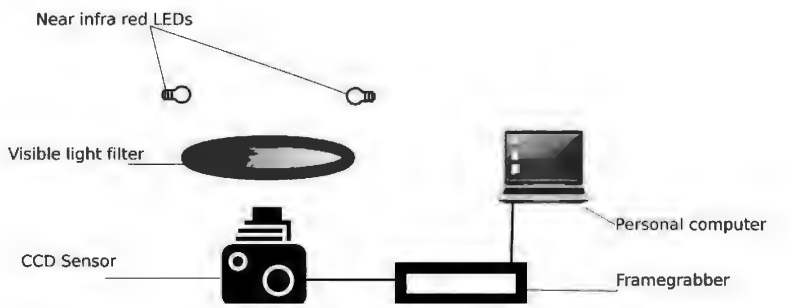

Fig. 2. Device schematics.

Fig. 3. Device prototype.

Discussed device prototype uses LED matrices that give continuous light. Creation of a triggered solution in order to obtain impulse driven LED matrices is a possibility worth investigating. This solution would provide better lighting conditions due to the fact that impulse driven LEDs can handle greater current values: $300mA$ instead of $150mA$ for $100\mu s$ which results in higher luminance.

2.3 Image acquisition subsystem

Image acquisition subsystem consists of CCD sensor and frame grabber (connected to a personal computer). At this stage of development there is no correlation between lighting subsystem triggering and image acquisition subsystem. The next step is to implement self-calibration algorithm which would, basing on measuring lighting conditions, control luminance of LED matrices. This would provide pre-acquisition normalization of captured scene.

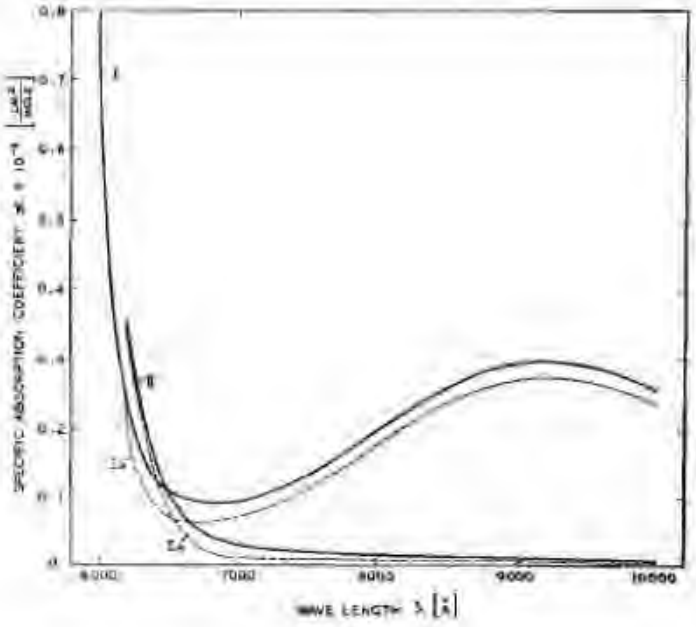

Fig. 4. Absorption spectra of HbO_2 (I, Ia) and HbCO (II, IIa) in the infra red region. This figure comes from [6].

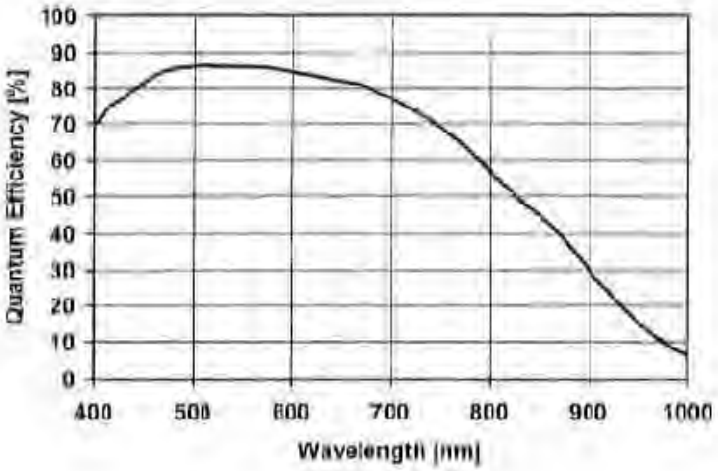

Fig. 5. Typical QE for back-illuminated backside-thinned CCDs. This figure comes from [7].

Obtained gray scale image of finger veins is presented in Fig. 6 .

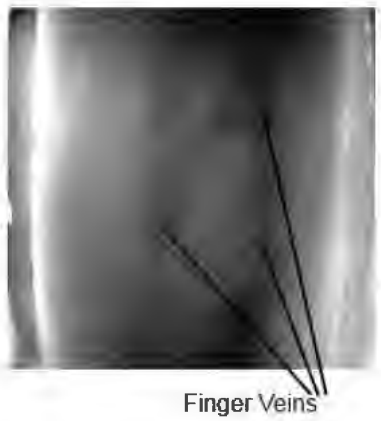

Fig. 6. Obtained finger vein image.

Dark shapes in central region of the picture are the discussed veins.

3 Biometric authentication system concept using device prototype

3.1 Overview

There are two main operation modes for biometric authentication system representing respective processes. First of them is enrollment mode in which biometric templates are obtained, connected to personal data and stored into database. Second is verification in which biometric template is obtained and matched against data stored in database. In the following sub sections, a brief description of both is presented.

3.2 Enrollment

Enrollment process, as presented in Fig. 7, Below, a short description is given:
1. Process starts with vein image acquisition;
2. Image is normalized;
3. Vein pattern is extracted;
4. Template is stored to database.

System user initiates the enrollment action and puts his or her finger on the device for scanning. System should recognize, if obtained template

is of good quality. If it is, obtained pattern is encapsulated into template along with subject's personal ID and finger ID. After template creation, it is stored into database. System should provide feedback whether enrollment was successful or not (FTE).

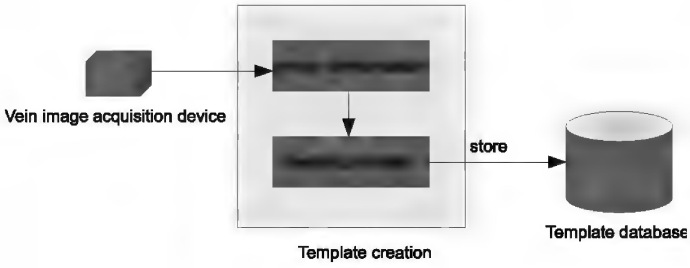

Fig. 7. Enrollment block diagram.

3.3 Verification

Block diagram of a verification process is presented in Fig. 8.This process consists of the following steps:
1. Process starts with image acquisition;
2. Image acquisition is followed by image normalization;
3. Operating on normalized image, features are extracted.
4. With vein pattern extracted, template is matched against corresponding user's finger template retrieved from database by both personal ID and finger ID.

System user initiates the verification action and puts his or her finger on the device for verification. System should recognize, if obtained template is of good quality. If it is not, user should be informed of image acquisition error (FTA). Verification result should be unambiguous presenting either verified user credentials or — if obtained template X_Q differs from X_I — information on non-match decision.

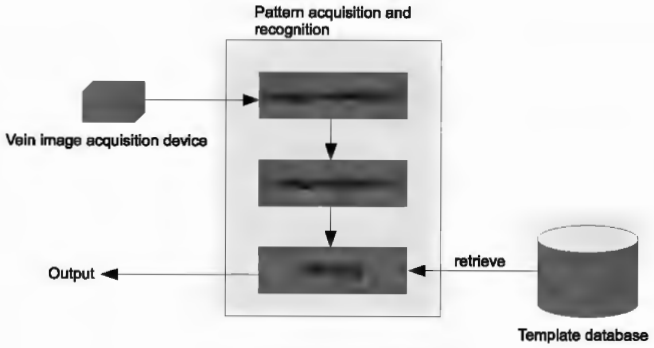

Fig. 8. Authentication block diagram.

3.4 Feature extraction

Repeated line tracking algorithm (as presented by Miura at el. [2]) was chosen for implementation as a reference method. The following symbols and variables are used in the algorithm description:
- let R_f be the image subspace inside the finger outline;
- let $F(x_i, y_i)$ be the value of the i-th pixel;
- let (x_s, y_s) be the starting point coordinates; $(x_s, y_s) \in R_f$;
- let (x_c, y_c) be current tracking point coordinates; $(x_c, y_c) \in R_f$;
- let D_h be a parameter to indicate horizontal movement direction:

$$D_h = \begin{cases} (1,0) & \text{if } r_{nd}(2) < 1 \\ (-1,0) & \text{if } r_{nd}(2) \geq 1; \end{cases} \tag{5}$$

- let D_v be a parameter to indicate vertical movement direction:

$$D_v = \begin{cases} (0,1) & \text{if } r_{nd}(2) < 1 \\ (0,-1) & \text{if } r_{nd}(2) \geq 1; \end{cases} \tag{6}$$

where $r_{nd}(n)$ is a random uniform distribution number: $0 \leq r_{nd} \leq n$;
T_c is a space containing all previous tracking points (after [2] — locus table); N_c is a space of potential achievable tracking points defined as:

$$N_c = T_c' \cap R_f \cap N_r(x_c, y_c). \tag{7}$$

$N_r(x_c, y_c)$ is a set of neighbor points of current tracking point (x_c, y_c) defined as [2]:

$$N_r(x_c, y_c) = \begin{cases} N_3(D_h)(x_c, y_c) & \text{if } r_{nd}(100)p_h \\ N_3(D_v)(x_c, y_c) & \text{if } p_h + 1 \leq r_{nd}(100) < p_h + p_v \\ N_8(x_c, y_c) & \text{if } p_h + p_v + 1 \leq r_{nd}(100). \end{cases} \quad (8)$$

Moreover:

N_3 is a set of three neighbor points;

N_8 is a set of eight neighbor points of the current tracking point;

p_h - parameter reflecting probability of electing three neighbor points in horizontal direction ($p_h \in < 0, 100 >$);

p_v - parameter reflecting probability of electing three neighbor points in vertical direction ($p_v \in < 0, 100 >$);

- let V_l be the parameter evaluating the next possible current tracking point

$$\begin{aligned} V_l = \max_{(x_{c'}, y_{c'}) \in N_c} \{ & F(x_c + r\cos\theta_{c'} - \tfrac{W}{2}\sin\theta_{c'}\ , y_c + r\sin\theta_{c'} + \tfrac{W}{2}\cos\theta_{c'}) + \\ & + F(x_c + r\cos\theta_{c'} + \tfrac{W}{2}\sin\theta_{c'}\ , y_c + r\sin\theta_{c'} - \tfrac{W}{2}\cos\theta_{c'}) + \\ & - 2F(x_c + r\cos\theta_{c'}\ , y_c + r\sin\theta_{c'}) \} \end{aligned} \quad (9)$$

where:

W is width of the vein's color-depth profile;
r is radius of the aforementioned profile;
$\theta_{c'}$ is an angle between line parallel to x axis passing through the current tacking point (x_c, y_c) and line segment originating in the current tracking point and ending in the potential tracking point $(x_{c'}, y_{c'})$.

Graphical representation of the above mentioned variables is given in Fig.9.

- Let T_r be the cumulative locus space for repetitive line tracking.

The algorithm:

Step 1. Determine starting point of the algorithm.

Starting point $(x_s, y_s) \in R_f$ is chosen using Monte Carlo method. The starting point is now the current tracking point (x_c, y_c).

Step 2. Detect tracked line direction and move current tracking point:

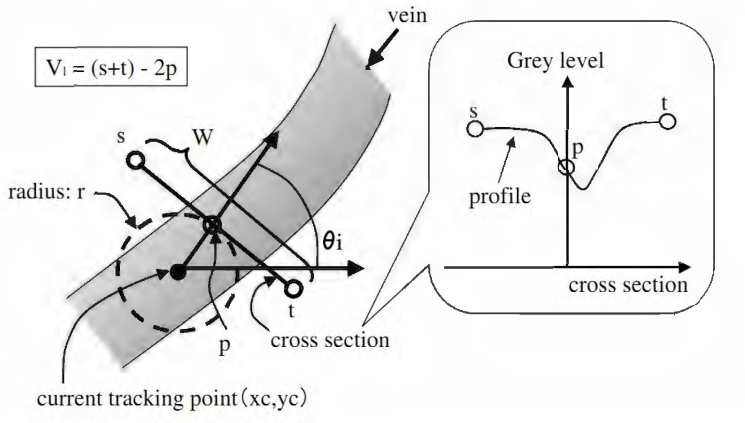

Fig. 9. Dark line detection. This figure comes from [2].

T_c is initialized. N_c is calculated. Then, direction of the tracked line is detected by repetitive calculation of the V_l value for pixels which are in N_c set. A new current tracking point $(x_{c'}, y_{c'})$ is chosen for the maximal value of V_l and a previous tracking point is stored into T_c. Repeat until V_l is negative.

Step 3. Update cumulative locus space

T_r is updated with elements of T_c.

Step 4. Repeat steps 1—3

Steps 1—3 are repeated for a previously established number of times n_{rep}.

Step 5. Spacial reduction of the template obtained and storage.

The resulting locus space T_r is binarized using threshold value and read in non-overlapping blocks of size $n_{red} \times n_{red}$. The n_{red} parameter is chosen experimentally depending on input image resolution.The reduced locus space $T_{r'}$ is created by storing the average values from each block. $T_{r'}$ is then rebinarized using multiple threshold method to create three classes of points: background, ambiguous region and veins. Template $T_{r'}$ is stored into template database.

This algorithm is used to acquire a single template of a single finger. In order to obtain lower FRR values during verification process, there often are several templates of a single finger acquired. These templates differ because of variable finger positioning during enrollment. Verification against multiple templates causes verification process time to be longer. This causes inconvenience for system's users. In order to shorten verification time, following modification to the algorithm is proposed:
- let n be the number of subsequently obtained vein patterns of a previously determined finger; $n \in \mathbb{N} : n > 0$;
- let $X_{I_1}...X_{I_n}$ be a family of templates of a determined finger I.

The goal is to find the mean template $X_{I_{mean}}$ to be stored into template database as a reference template. Evaluation of the proposed method should be carried out by comparison of FAR, FRR parameters for original and modified feature extraction methods and template matching time t_m.

4 Conclusions

In this article, a short description of a biometric system concept is given. Vascular biometrics concept is discussed. This is followed by commercial systems implementation description as observed in financial sector in Poland.

Next section describes vein pattern acquisition device designed by the author focusing on two main subsystems of the device: lighting subsystem and image acquisition subsystem. Also, description of biometric authentication system utilizing created prototype is given. Reference feature extraction algorithm is described.

Author identified key directions for future investigation. These include:
- Device prototype:
  - triggered lighting subsystem (impulse driven LED matrices);
  - lighting subsystem self–calibration algorithm basing on image histogram analysis;
- Feature extraction:
  - calculation of a mean template from multiple enrollment processes;
  - selection of a template matching algorithm.

References

1. Jain, A. K., Ross A., Prabhakar S. (2004) An Introduction to Biometric Recognition, *IEEE Transactions On Circuit And Systems For Video Technology, vol. 14, No. 1*, 4-20.

2. Miura N., Nagasaka A., Miyatake T. (2004) Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, *Machine Vision and Applications 15*, Springer-Verlag, Berlin, Germany 194-203.
3. Himaga M., Kou K.(2008) Finger Vein Authentication Technology and Financial Applications*Advances in Biometrics*, Springer, London, UK 89-105
4. Chang S., Larin K. V., Mao Y., Flueraru C., Almuhtadi W. (2011) Fingerprint Spoof Detection Using Near Infrared Optical Analysis, *State of Art in Biometrics*, InTech, Rijeka, Croatia 57-84.
5. Wang K., Ma H., Popoola O. P., Li J. (2011) Finger Vein Recognition, *Biometrics*, InTech, Rijeka, Croatia 29-54.
6. Horecker, B. L. (1943) The absorption spectra of hemoglobin and its derivatives in the visible and infra-red regions, *Journal of Biological Chemistry, 148*, Rockville, Maryland, 173-183.
7. Tower, J. R. et al.. (2003) Large format backside illuminated CCD imager for space surveillance, *IEEE Transactions On Electron Devices, vol. 50, issue 1*, 218-224.

Systemy biometryczne - koncepcja oraz akwizycja obrazu dla pozyskania wzorców naczyń krwionośnych palca

Streszczenie. W niniejszej pracy zawarto zwięzły opis systemu biometrycznego, prezentując aktualne rozwiązania komercyjne dla sektora finansowego. W dalszej części pracy zaprezentowano prototyp urządzenia służącego do akwizycji obrazu naczyń krwionośnych palca. Pracę kończy propozycja systemu uwierzytelnienia biometrycznego. W *Podsumowaniu* wskazano kierunki dalszych badań.

ISBN 9788389475442