Security Information System, Based on Fingerprint Biometrics

Komlen Lalović

ITS–Information Technology School, 34 Cara Dušana Street, 11080 Belgrade, Serbia, komlen.lalovic@its.edu.rs

Ivan Tot

University of Defense, 33 Pavla Jurišića Sturma Street, 11000 Belgrade, Serbia, ivan.tot@va.mod.gov.rs

Aleksandra Arsić

Mathematical Institute, 36 Kneza Mihaila Street, 11001 Belgrade, Serbia, aleksandra@mi.sanu.ac.rs

Milan Škarić

Enon Solutions, 86 Omladinskih Brigada Street, 11070 Belgrade, Serbia, milan@enonsolutions.com

Abstract: This work presents a novel security information system based on fingerprint biometrics. It combines cancelable biometrics, security algorithms such as RSA and AES, both synchronous and asynchronous for data encryption. By implementing novel devices developed on the Raspberry Pi Platform and wireless communication, 100% accuracy in real terms, will be enabled and FAR and FRR will be decreased to a minimum - as it were, zero. At the core of the information system are devices and software algorithms implemented for biometric identification of maternity, as a dual fingerprint scanner that provides data of mother and new born baby fingerprints and in the further process, guarantees maternity of a new born baby with 100% accuracy. All this is developed as a novel method of identity determination, based on baby fingerprint minutiae, instead of current systems that are prone to many errors. This system will prevent any possible replacement or identity theft in every maternity ward.

Keywords: Biometric; Fingerprint; Security; Software; Information system

1 Introduction

This paper presents work in the field of advanced security systems, widely used in modern society and in protection systems. Biometry is the scientific discipline and techniques for measuring and analyzing biological characteristics of people.

We have solved the issue and societal problem of the timely determination and logging of a newborn babies minutiae, thereby protecting them with a crypto algorithm enrolled with cancelable biometrics. Our information system prevents any possible theft or misplacement of the baby's identity, providing 100% accuracy in its determination and showcases a device which scans, stores the encrypted personal data, with one goal - to provide validated parenthood for each newborn baby, in a crowded hospital.

The information system (IS) completely removes the fear that almost every mother has during birthing, and it also removes the question "Have I brought home my baby… for sure?". This method presents a new implementation of information technology security in the public health system and raises it to a new level.

It also links the patented device for biometric identification of newborn babies with two existing software algorithms and the necessary writing procedures, so that this new approach can be carried out. Not only does it solve a huge problem - possible theft or misplacement a newborn baby's identity, but it also removes a fear that women have, when giving birth.

This is not just problem in Serbia, it is global problem, baby switching has happened in almost every country in the world. According to Brandon Gille, USA study, of 4 million new born babies, 28,000 from them had been misplaced! [20]

There are no similar solutions at this time. There is some attempts to solve this kind of problem, with foot prints, in USA, but it is an ink print not digitally processed.

2 Problem Solving

The information system possesses two main software algorithms that will be presented herein and which provide all of the device functionalities. These functionalities will be illustrated in figures, which point out how our model was built, designed and developed. The paper will present possible advantages and benefits that are a qualitative leap in the public health care system, precisely in maternity wards all over the world.

By implementing this new system, it is possible to establish a Wi-Fi communication and storage types, for fingerprints scanned from both the mother and the baby together at the moment of birth, and to generate a unique identity reference which is encrypted and will guarantee parenthood over every newborn baby with 100% accuracy. Wi-Fi is required during scan process or a cable connection within 30 minutes of scanning, since device has a data store timeout for those 30 seconds because of security issues.

Considering experiment, results have been presented and listed in several publications, where most relevant is under SJEE. It contains experiment with newly born baby and the scan process of all hand fingers with different type of scanners. [5]

This invention belongs to the field of Applied Information Technology. Biometrics systems and device with its functionality is similar and close to a dual fingerprint scanner with two fields - first the scanning process takes place (both the mother's and the baby's fingers), then the device makes a unique reference which will be the ID for each mother/baby relationship for every newborn baby in the hospital.

3 Technical Overview

The main technical problems which are solved by this IS are the following:

The design and development of a new device based on our patented device [11] incorporates a dual fingerprint scanner, for scanning fingers of both the mother and the baby at the moment of birth. The device cross view will be similar to the current classic fingerprint scanners; therefore, the tablets would have two fields for scanning fingers of two different people (the mother and the baby). After this process, the device will encrypt and store the data. The device cross view is given in the following pictures.

The real technology improvement and contribution is that the device is highly practical and easy to use and control. The maintenance of the device is easy, classic and similar to other fingerprint scanners. Beside its common purpose and scanning two fingers of different people at the same time, it will provide a unique ID reference (like Primary Key PK) which will be the basis for every pair of the scanned mother and baby.

The realized information system (IS) presents the optimal solution for this type of work, which defines the strict procedures that need to be followed. The IS will also implement the IT technology in the public health system. Current biometric devices can scan one or more fingers from **one** person, then repeat with another, but there are no fingerprint scanners which may scan fingers of two different

people at the same time on a single device. Especially, there are no devices that may make a unique reference while scanning, which will further be connected to the record of scanned fingerprints previously stored data. [4] [7]

This is provided by the **Device for biometric identifying of Maternity,** in the functionality development of which the encrypted data that will carry information about two people (the mother and the baby) and the linked unique ID reference will be implemented.

Our device has two fields for scanning fingers of two different people at the same time. This is crucial improvement in the technology for solving problems.

However, the question that may emerge concerns the time-saving feature needed for the process scanning of both people and all of the back-end Information Technology (*IT*) in background, of the future system that now is now scanning for one person.

Our device provides improvements in economy and the time spent during the process of scanning, enabling the possibility for reduction of costs for each new device, with the advantage of less time needed for processing data obtained from the image of the finger scanner. The device provides the optimal solution for resource usage in the case of processing data acquired during the process of fingerprint scanning, primarily considering the memory usage and activity of the Central Processing Unit (*CPU*). Figure 1 presents a completely new information system with devices and communication. All devices are synchronized with the server and database which stores the data, using cancelable biometrics and using a cable or wireless connection. Devices do not communicate one to another.

Figure 1
Information system and communication between components

4 Information System

The Information System created for this new baby identification method, based on the fingerprints, consists of obtaining, encrypting, storing and verifying data. The next step follows the procedures that need to be performed. Figure 2 shows the Class diagram for this Information System.

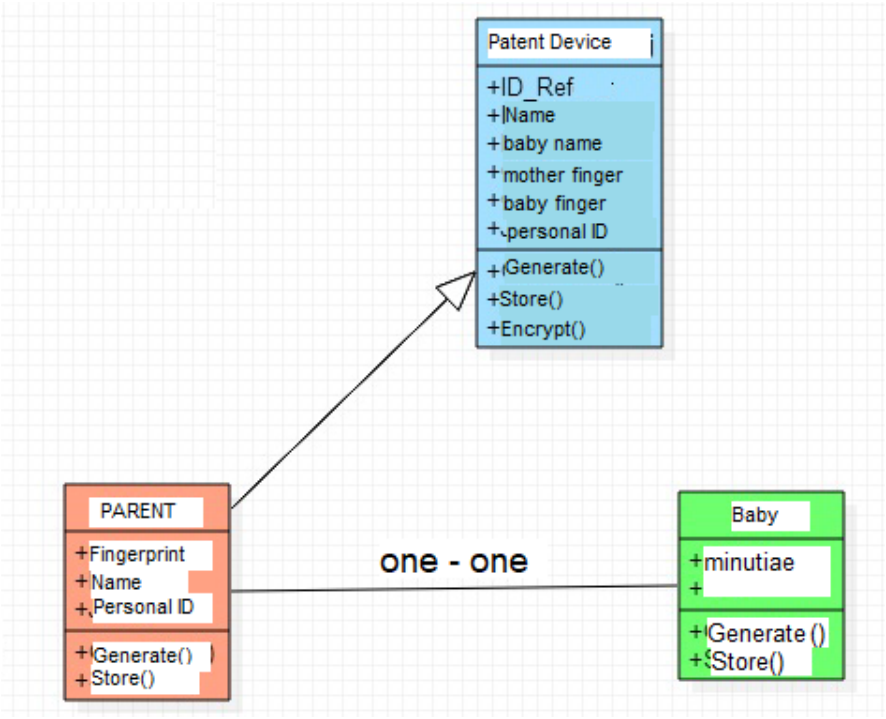

Figure 2
Class diagram of Information system

4.1 Can Baby Fingerprints Be Obtained?

The device that we have invented has features, such as, a real time dual biometric fingerprint scanner that has two fields for scanning fingerprints of the mother and the baby or two and more, at the very moment of birth. The first field is larger, with classic scan resolution of 500 dpi; the second field is physically smaller but has larger scan resolution – a minimum of 1000 dpi, so it can produce scans of a the baby's fingerprint, that is relatively small. [8] [12] [13]

Our research is based on the scientific fact that human fingerprints are formed during the prenatal period for every fetus/baby and that they remain constant in shape of minutiae during the entire life of the individual. [1] [3] [9] [10]

The most important fact to mention, is that babies who are born prematurely, during the 8th and especially by the end of the 7th month of pregnancy, have formed fingerprints on the finger of both hands. This is the starting point of our research. [1] [5] [16] [18]

Considering this scientific fact, which is crucial for our patent and this device, this research and this project realization will provide a qualitative jump in gynecology, midwifery and nursing in every hospital in the entire world. We need to provide 100% accuracy and guarantee the maternity over a newborn baby anywhere in the world. We achieve this by placing one of the baby's fingers on the smaller field of our device simultaneously with the mother's finger on the larger field of the device and initiating the scans. At this point, the device also generates a unique reference for this pair of scanned data-minutiae (mother and baby). Later, after a few days, when parents leave the ward, the next step is to check the fingerprint on the same device, which should confirm the baby's identity. This procedure will provide new quality and it will prevent any possible misplacements or baby theft. [1] [2] [6]

Figure 3 presents the final results of the empirical test results, made of a new born The results presented here are an absolute novelty in fingerprint biometrics.

Attempt / Scanner type	Optical	Capacitive	Preasure	Thermal
Finger 1	10	7	3	2
Finger 2	10	6	2	2
Finger 3	10	6	2	1
Finger 4	10	5	1	0
Finger 5	9	4	0	0
Percentage of success	98.00%	56.00%	16.00%	10.00%
Total	49	28	8	5

Figure 3

Results of research and experiment enrolled per each finger and each scanner type

When it comes to other biometrics, such as iris recognition, they did not prove to be as useful, since they are unstable on babies. The reason lies in the fact that iris and eye pigmentation is not formed until 4 years of age, and it keeps changing in shape and in color. Therefore, it cannot be used for this purpose. [5] [11]

Other body parts, especially palm or other limbs, cannot be used because they rapidly change due to the normal process of growing up. This is the reason why this excellent, scientific fact concerning fetus fingerprints, their prenatal formation, by the end of the 7^{th} month to be precise, in the pregnant mother, and their minutiae construction remaining unchanged, is marvelous and useful. [1] [6]

Mothers-to-be, as well as, medical staff in maternity wards, in health care facilities, have many different concerns, during the birthing process. A study that was carried out in Australia and New Zealand, by the Woman and Birth Journal, in 2009 included 17 different workshops, with more than 700 midwives, over a period of 5 years, points out that women had 144 various fears at the moment of giving birth. Taking this fact into consideration, our device can prevent a great deal of those tremendous fears and perhaps eliminate them in a total number of n=43. [6]

We have to mention that all the data obtained, from the mother and baby, during the process of fingerprint scanning, together with the unique ID reference encryption and storage in the device memory and/or on a server in the encrypted forms never leave the device in vulnerable state, or available to the public. The data is only to authorized nurses, doctors and midwifes in the maternity ward. [5] [6]

4.2 Improvements in The New Information System

The new IS combines device for biometric identification of newborn babies based on the fingerprint scan will enable the following:

- Improvement and evidence of maternity for every newborn baby
- Exclusion of any possible replacement or identity theft of newborn babies
- Safety for each parent couple
- Portability due to the small dimensions and low weight; it is ambient friendly and does not pollute environment
- A good ratio of price/quality
- A wide range of applications and use

In order to understand better the functionality and application of the device, as well as its practical realization, there are a few pictures that illustrate the device and algorithms, long with the cross-section of the patented device.

Figure 4 illustrates the device for biometric identification of maternity in a completely new view with digital display, a switch and two fields for fingerprint scanning.

Figure 4 contains the following remarks:

B Body of the device

I Power switch with two positions (on/off)

D Device display for displaying all the details, such as a unique ID reference generated during the process of scanning

S Set button for starting the scanning process and reading parameters obtained by fingerprint scanning

R Reset button

R1 Command button that saves and stores data

S1 Field for scanning the fingerprint of the baby's finger, smaller than the field for scanning the mother's fingerprint

S2 Field for scanning the fingerprint of the mother's finger, larger field

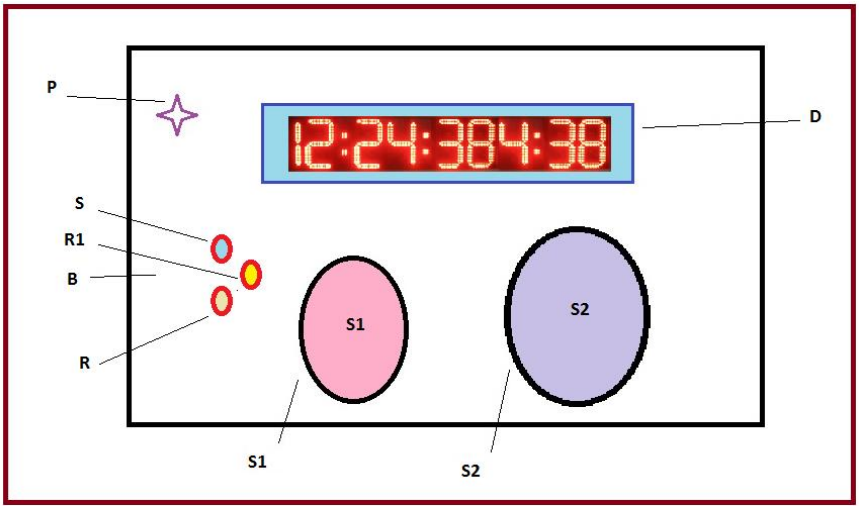

Figure 4
Detail description of device functionality

5 Acquiring Software Algorithm in Pseudo Code

The algorithm, in pseudo code, is listed here, in order to illustrate the logic and all possible software features that the device possesses, to explain in details how the entire system is supposed to accomplish its purpose of providing a completely new quality implementing information technology. [11]

```
---------------------------------------------------------------------------
Line 01     START
Line 02     BEGIN LOOP 1 TO 3
Line 03     FIELD-1 SCANN
Line 04     IF F1 OK
  THEN GOTO GENERATE UNIQE ID
                          ELSE IF LOOP < 3 GOTO END
Line 05     BEGIN LOOP 1 TO 3
Line 06     FIELD-2 SCANN
Line 07     IF F2 OK
   THEN GOTO GENERATE UNIQE ID
                            ELSE IF LOOP < 3 GOTO END
Line 08     GENERATE UNIQE ID REFERENCE
Line 09     GENERATE PIN CODE
Line 10     ENCRYPT DATA
Line 11     GENERATE HASH VALUE
Line 12     STORE AND SAVE DATA
Line 13     DISPLAY SUCCESS MESSAGE
Line 14     FINISH
---------------------------------------------------------------------------
```

Figure 5 represents the device algorithm, that is main software part of our innovative device and it can provide the process functionality with the deduction process. After the scanning process, it generates unique ID, encrypts those data and generates a hash value providing information about a successful scanning event.

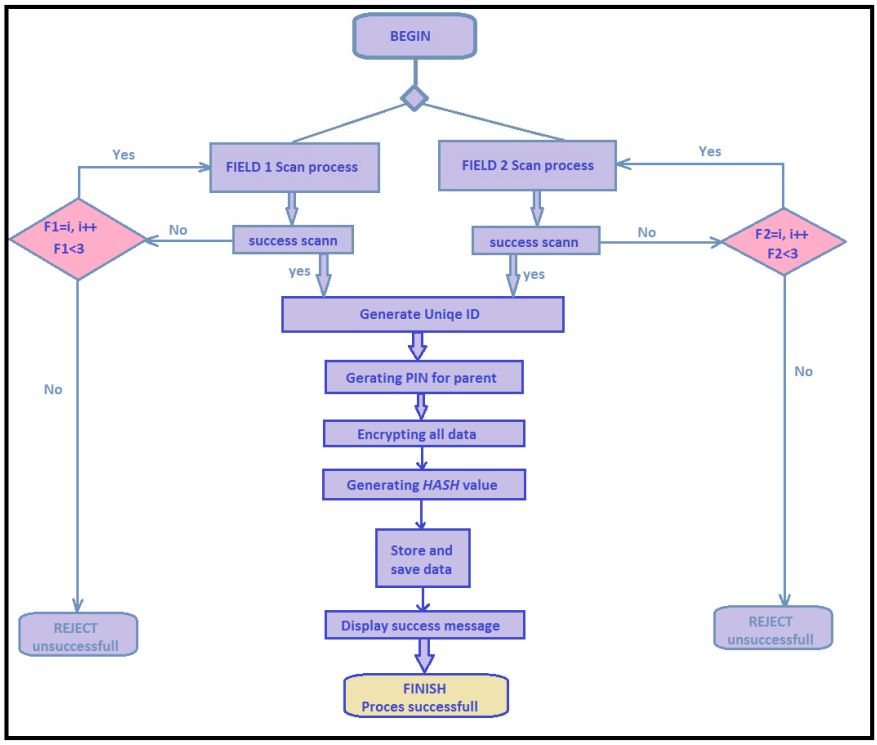

Figure 5
Device software algorithm for data acquisition

6 Verification Software Algorithm in Pseudo Code

This algorithm in pseudo code illustrates the logic and all possible software features that the device possesses for the verification of fingerprint minutiae and explains how the system uses cancelable biometrics to enable security and private data. [11]

Figure 6 represents the essence of this device algorithm which is a part of our innovated device and which provide the process functionality to verify stored data. It has a double check to provide total security of its functionalities. It compares encrypted data and also check the hash value of a stored data.

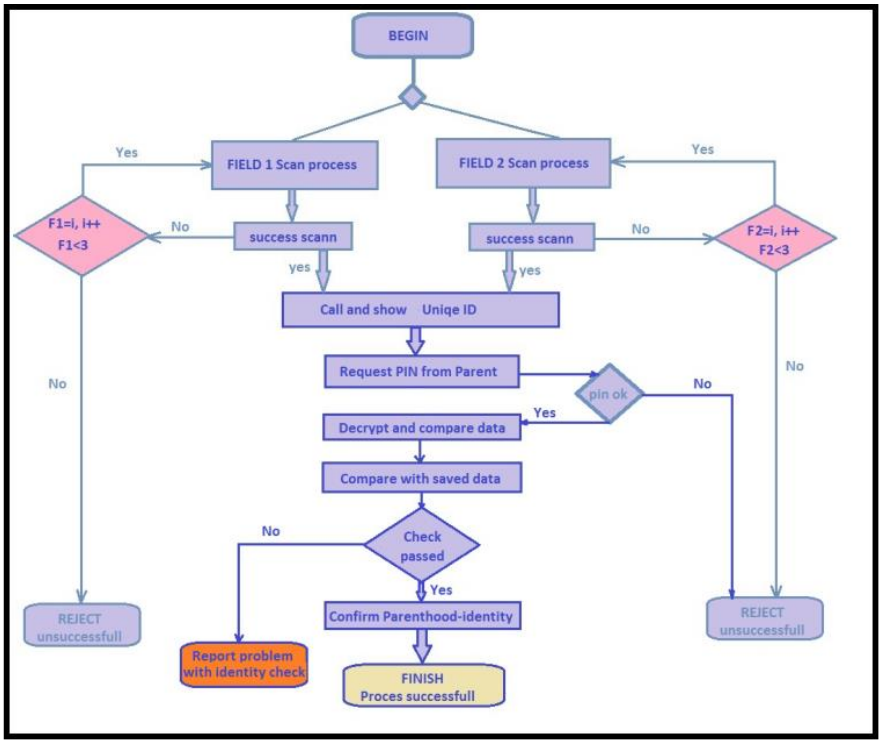

Figure 6
Device software algorithm for data verification

7 Possibilities of Further Development

The Information System with the device and novel method of implementing the new device, with biometric fingerprint identification of maternity and scanning each newborn baby can be used as a brand new model, in the public health care systems. Considering further development of similar fingerprint biometrics system in everyday care, hospitals may solve various problems, regarding moving small children and their continuous monitoring. It is necessary to provide further development and research based on the patented device, innovation and qualitative research that were performed during this study.

Software algorithms given herein, will improve the device functionality and enable it to work faster. They can be used as a part of much larger health care system, regarding young children and their pediatric care; they can also provide basic data concerning possible allergies and specific health states for each child.

Combinations may allow for great improvements in that part of the health care system at a global level.

Conclusion

This novel device combines the objectives of three parts: the patented device, the information system and a safe maternity ward approach. It can improve the level of public health in the Republic of Serbia. The system is modular, it can be updated and, most importantly, it can be the basis for future developments in biometric systems. The device can be applied in a number of countries, to fight the organized criminals and help to prevent the theft or misplacement of newborn babies, especially in territories with a low IT infrastructure and technological development.

Every kind of biometry is eager to minimize both FAR[1] and FRR[2] in order to be much more accurate and secure. This device has accomplished this, since it combines two scanned data and its accuracy grows exponentially. In the modern IoT (Internet of things), the majority of countries try to provide a completely new quality of health care service, help the staff in maternity wards, make the process of giving birth much easier and more relaxed, both for mothers-to-be, gynecologists, midwifes and nurses.

Conflict of Interest

None.

Acknowledgement

We want to thank every single person and baby involved into this research with purpose to improve IT in public health system.

References

[1] Anil K. Jain-*Michigan State University*, USA, Patric Flynn-*University of Notre Dame, USA*, ARUN A. ROSS-*West Virginia University, USA* (2008)*:* Handbook of Biometrics – Sringer, USA

[2] Komlen Lalović, Nemanja Maček, Milan Milosavljević, Mladen Veinović, Igor Franc, Jelena Lalović, Ivan Tot - Biometric Verification of Maternity and Identity Switch Prevention in Maternity Wards, Acta Polytechnica Hungarica, Volume 13, Issue Number 13, 2016 DOI: 10.12700/APH.13.5.2016.5.4

[3] NIST, *A Survey of Access Control Methods*

[4] Nemanja Maček, Borislav Đorđević, Jelena Gavrilović, Komlen Lalović - An Approach to Robust Biometric Key Generation System Design, Acta

[1] FAR – False Accept Rate

[2] FRR – False Reject Rate

Polytechnica Hungarica, Volume 12, Issue Number 8, 2015, DOI: 10.12700/APH.12.8.2015.8.3

[5] Komlen Lalović, Milan Milosavljević, Ivan Tot, Nemanja Maček: Device for Biometric Verification of Maternity, Serbian Journal of Electrical Engineering-Vol. 12, No. 3, October 2015, DOI: 10.2298/SJEE1503293L

[6] Hannah Grace Dahlen, Shea Caplice: "What do midwives fear?", Published Online: July 24, 2014 – Elsevier, *Women and Birth, Journal of Australian College of Midwives*

[7] Komlen Lalović, Ivan Tot, Svetlana Andjelić - How to Guarantee Baby Identity based on Fingerprint Biometry, Bisec 2017 - International conference in Security ICT, October 18th-Belgrade, Serbia

[8] Komlen Lalović, Jasmina Nikolić, Ivan Tot, Žana Lalović - Software Algorithm of Device for biometric identification of Parenthood, BISEC 2016 - International conference in Security ICT, October 15th-Belgrade, Serbia

[9] Keith Moore, T. V. N. Peraud, Mark Torchia: Before We Are Born, Elsevier UK, Saunders, ISBN: 9780323313377, 2014, 9th Edition.

[10] NIST publishes compression guidance for fingerprint, Journal Elsevier - Biometric Technology Today, Volume 2014 Issue 4, April 2014, Pages 12

[11] Komlen Lalović, Patent Overview: Device for Fingerprint Identity Guarantee - Military Technical Courier, 2018, Vol. 66, Issue 2, http://dx.doi.org/10.5937/vojtehg66-15868

[12] Chouaib Moujahdia, George Bebisb, Sanaa Ghouzalic, Mohammed Rziza: Fingerprint shell: Secure representation of fingerprint template,and Pattern Recognition Letters, Volume 45, 1 August 2014, pp. 189-196

[13] Chungkeun, L., Hang, S. S., Jongchul, P., Myoungho, L. The optimal attachment position for a fingertip photoplethysmographic sensor with low DC. IEEE Sens. J. 2012;12:1253-1254

[14] Elgendi, M. On the analysis of fingertip photoplethysmogram signals. Curr. Cardiol. Rev. 2012;8:14-25

[15] Martti Juhola, Youming Zhang, Jyrki Rasku: Biometric verification of a subject through eye movements, Computers in Biology and Medicine, Vol. 43, Issue 1, pp. 42-50, Published in issue: January 01, 2013

[16] Jan Evangelista Purkynje (1787-1869): First to describe fingerprints, Andrzej Grzybowski, Krzysztof Pietrzak, Clinics in Dermatology, Vol. 33, Issue 1, pp. 117-121, Published in issue: January, 2015

[17] Esperanza Gutiérrez-Redomero, Noemí Rivaldería, Concepción Alonso-Rodríguez, Ángeles Sánchez-Andrés: Assessment of the methodology for

estimating ridge density in fingerprints and its forensic application, May 2014, Volume 54, Issue 3, pp. 199-207

[18] Kimberly Kaplan-Sandquist, Marc A. LeBeau, Mark L. Miller: Chemical analysis of pharmaceuticals and explosives in fingermarks using matrix-assisted laser desorption ionization/time-of-flight mass spectrometry, Forensic Science International, Vol. 235, pp. 68-77

[19] Lynsey Nicholson, Kevin Farrugia, David Bremner, Dennis Gentles: A preliminary investigation into the acquisition of fingerprints on food Sarah Ferguson, Science and Justice, Vol. 53, Issue 1, pp. 67-72

[20] https://brandongaille.com/20-babies-switched-at-birth-statistics

[21] https://patents.google.com/patent/WO2016036267A1/fi