

Device for Biometric Verification of Maternity

Komlen Lalović¹, Milan Milosavljević¹, Ivan Tot², Nemanja Maček³

Abstract: Biometry is the scientific discipline and technology that measures and analyzes physiological or behavioral characteristics of people and is widely deployed in modern society security systems. Device for biometric identification of maternity is a dual fingerprint scanner that acquires fingerprint templates of the mother and the child at the very moment of birth, generates unique ID reference, and further guarantees mother-child relationship with that reference. Technical issue that is solved with this work and the proposed device is scanning, processing, and storing encrypted biometric templates with a goal to provide a 100% guarantee maternity for each new born child. Scanning the fingerprints of both mother and the child simultaneously, at moment of birth, and pairing them with unique ID reference removes potential fears occurring from hospital negligence to malicious activities, while the data encryption raises the whole process to the highest level of security and confidentiality. The main contribution of the device that removes the fear that almost every mother has in this period as it provides an answer to the question: "Is this my baby?" with a 100% guarantee "It's certainly yours!"

Keywords: Biometry, Fingerprint, Minutiae, Child, Patent.

1 Introduction

Patented device for biometric identification of maternity has been invented with a goal to remove a shadow from possible events that occurred in many countries regarding stealing or mixing the identities of new born babies, thus preventing the fear that all future mothers have. The device makes the blissful moment of bringing new life to this world for gynecologists, midwives and nurses as well.

This paper presents all the functions that the device possesses. The figures show how the model is made, how cross-state looks like, how it is constructed and implemented, what are the possible advantages and benefits and what is a qualitative leap in Health Care system, precisely in maternity hospitals

¹Singidunum University, Danijelova 32, 11000 Belgrade, Serbia;
E-mails: mmilosavljevic@singidunum.ac.rs; komlen.lalovic.13@singimail.rs

²University of Defense Rep. of Serbia, Generala Pavla Jurisica Sturma 33, 11000 Belgrade, Serbia;
e-mail: ivan.tot@va.mod.gov.rs

³SECIT Security Consulting, Aksentija Maksimovića 21, 26000 Pančevo, Serbia;
E-mail: nmacek@secitsecurity.com

worldwide. Fingerprints of mother and a new born child are scanned at the moment of birth simultaneously, the unique ID reference is generated and the data is further encrypted. The data stored internally on the device or on a remote server provides a 100% full proof maternity guarantee for each new born child.

This invention, and the concrete device is realized as a dual fingerprint scanner that scans two fingers at the same time (mother and child), generates a unique Identification (ID) reference and further uses that reference to verify “mother-child relationship” for every newborn in maternity hospitals [1].

According to the International classification of Patents, this patent is classified as G06F21/00: biometric systems – devices for fingerprint scanners.

2 Technical issues

The technical issues which need to be solved with this Patent consist of:

- Construction solution for dual biometric fingerprint scanner for scanning fingers of a mother and the child, right at the moment of birth – during the first baby’s moments on this world. This device will be slightly different from the existing classic fingerprint scanners, i.e. it would have two fields for scanning fingers of two different persons [2].
- The device should be really effective during its work. The device is highly practical and user-friendly, easy to control and manipulate with. Maintenance is easy, classical and similar like the one for other fingerprint scanners.
- Besides its common purpose and scanning two fingers of different persons at the same moment it needs to provide a unique ID reference (similar like primary key) which will be used to pair scanned mother-child fingerprints [3].

3 Technology Review

Nowadays there are well known fingerprint scanners that employ different algorithms and methods in their process or work to determine the identity of individuals.

Having searched through the National base of Patents we have not found similar devices with the same purpose: dual biometric scanners that contain their own lightening, battery supply and encrypted wireless communication [4]. Existing devices scan one or more fingers of one person only, we are emphasizing the fact that it is only one person, and there are no scanners that scan fingers of two different persons at the same time using one device, especially not devices which make unique ID reference during scanning which will be connected with the record of fingerprint scanned and stored data [1].

In the issued Patent confirmation II-2009/0253, International classification G 07 D7/12 (2008.04) a device named “Hand mobile device for checking travel and personal documents, reading biometric data and face recognition of persons which carry those documents” is described, the only function of the device is scanning the fingerprint of one person at one moment [4]. Also in the issued Patent confirmation 13848069.4 dated April 2, 2013, with remark WO2014059761 and classification G06F21/00, a classic scanner named “Fingerprint identification device” is completely described device which has a function of scanning and provides a data about the fingerprint of person (extractor software for minutiae) [4 – 6]. However, this device does neither has two fields for simultaneous scanning fingers of two different persons nor generates unique unchangeable ID reference that is an additional guarantee of a person’s identity and two fingerprint template relationship.

The question which is asked nowadays is: can fingerprint scanning provide and relate the data of two persons at the same time using only one device? Surely it can, and it can be done with the highest quality, which is going to be shown in this work and the presentation of the Patent: the device for biometric identification of maternity. Existing Patents and devices, and present scanners which are used today do not have similar functions, and the main thing they do not have is simultaneous fingerprint scanning of two persons. This scanner contains two fields for scanning two fingers of two different persons (a mother and the child) and instantly generates a unique ID reference that guarantees the record of fingerprints. This innovative device provides improvements in both economic way and time spent during process of scanning, as it provides lower price of each device and less time needed to processing scanned data. The device also gives an optimal solution for resource usage in case of processing data acquired during the process of fingerprint scanning, first of all considering memory usage and activity of microcontroller (CPU).

Finally, regarding all these benefits, both in hardware and software, the device provides a qualitative leap in the area of Health Care system in all the countries where it will be implemented.

4 The Essence of Innovation

The essence of this innovation is the possibility to generate a unique ID reference that provides a 100% guarantee the maternity of each newborn (an undeniable reference with the mother). Dual biometric scanner has two fields for scanning fingerprints of a mother and the child. Precisely, one field is larger with the classic scan resolution of 500 dpi and the second filed is physically smaller but with larger scan resolution – minimum 1000 dpi, as child’s fingerprint is very small [7 – 9].

A fact of science is that the fingerprint is formed during prenatal period for every fetus and stays constant in the shape of minutiae during whole life [10 – 11, 12]. According to many researches realized on fingerprints of fetus, ultra waves and biometry scanning the minutiae on each finger are formed by the end of 7th month of pregnancy. It is important to mention that babies who are born before regular time of birth, during 8th, and especially by the end of 7th month of pregnancy have fingerprint on each finger, both hands and foots fingers already formed [10, 14, 15]. This scientific fact is essential for this device, this research and the realization or the Project that will provide a qualitative leap in gynecology, midwifery and nursing in every maternity hospital all over the world.

The identity of a baby and maternity of newborn babies will be 100% guaranteed after the fingerprints of both mother and the child are scanned at the moment of birth, when mother meets her baby for the first time, doctors and midwives measure of baby's weight and height and clean one of the baby's fingers with appropriate liquid and put the finger on the smaller field of fingerprint scanner together with mother's finger that is on the larger field of scanner. At that moment, the device makes scanning and generates the unique ID reference for that pair (mother-child). That is the crucial essence and proves that the newborn baby is baby of that particular mother. After few days when mother and baby leave a maternity, the check is performed on the same device and the device confirms the baby's identity bounded by ID reference with identity of his mother. That procedure has a new quality prevention of any possibilities to make an error.

This is essential because minutiae points (the ridge and valley structure) are the only biometrics that is formed prenatally and are the only physiological quality that can be used for biometry identity verification. The whole idea for Patent innovation is based on this scientific fact confirmed by both biometrics as a branch of computer science and gynecology – midwifery as a branch of Health Care protection system [13, 16]. Other biometric verification systems, such as iris recognition are not applicable in this scenario. As an example, the pigmentation in children's eye is changing until age of four, thus making iris recognition unstable at this point [13, 17]. The head, hand and body shape and size are rapidly changing since they normally grow up so it is obvious that they cannot be used either.

There are a large number of various fears during birth process, both of mothers and people in medical care system in maternity hospitals. According to studies which were made in Australia and New Zealand from year 2009 until 2011 and 17 workshops with more than 700 midwives, this device can prevent a certain part of one of these – dealing with unknown [16].

The data received during the process of fingerprint scanning of a mother and the baby, together with unique ID reference is stored on the device's memory or on a remote server in encrypted form. The device is never to be left available for general population, but only for authorized nurses, medical doctors and midwives. During every next process of scanning when the confirmation of parenthood is required, the authorized representative person will be present while the mother enters the PIN code that will decrypt the data and verify the maternity. The alternation of stored data is disabled as strong cryptographic protection and cancelable biometrics (non-invertible transforms) provide authenticity and integrity of the stored templates.

At the moment when the family is planned to leave the maternity hospital, a final verification is performed. The device is scanning the mother and baby's fingers simultaneously, compares it with the existing encrypted data stored at the moment of birth and if the match is confirmed, they are allowed to leave the hospital. This removes a reasonable fear of every mother in moments like that, as well as the fear of nurses, doctors and midwives. Archiving the data is available upon mothers request after the final verification is performed and the family leaves the maternity hospital. That is the moment when proving the guarantee of maternity is no longer necessary.

It prevents any possible theft or replacing the baby's identity, which has unfortunately being probably happened at some places and parts of the world, especially in south-east Europe, in the Balkan regions and countries of former Yugoslavia. Now the device will guarantee, prove and serve as the evidence of maternity of newborn babies.

The inventor of the Patent has taken maternity symbolically because the maternal instinct is the strongest instinct in nature. As giving respect to that natural instinct the inventor has decided to compare a mother's fingerprint with the baby's and make a unique ID reference that no one could change nor delete in the device.

The application of the device is universal, on every continent and country, and there are no restrictions on the use. It requires basic IT equipment – a server and this patent device which is a dual biometric fingerprint scanner. The device is low-cost, effective and can be installed in every maternity hospital in each country.

5 Benefits that Device Provides

Device for biometric verification of maternity will:

- Provide 100% proof of maternity for every newborn baby
- Eliminate possibilities of replacing or stealing identities of newborn babies

- Provide safety for all future parents, especially for mothers during such an important moment of giving birth.

Device is developed to have compact construction and practical handling throughout the process. It has its own energy supply with batteries or an adapter connector with DC supply. It's small sized, low in weight and portable. And finally it is expected to have quite good price/quality ratio, to be ambient and environmental friendly.

6 Description of the Device

For the better understanding of the functionality and the application of the device, five figures are provided in this paper. Front view of the device is presented on Fig. 1.

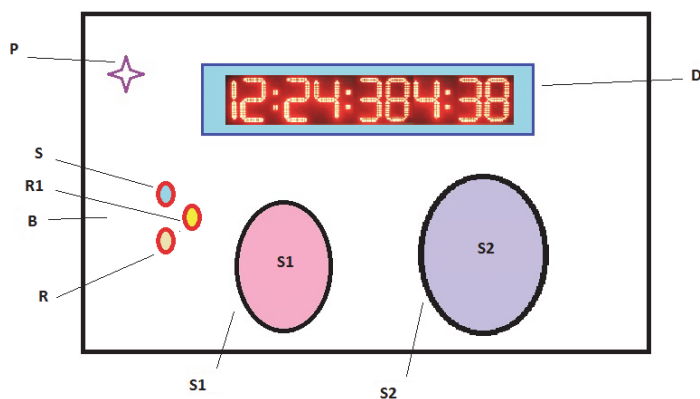


Fig. 1 – Device for biometric verification of maternity – front view.

The device consists of: body, ignition switch which can be in two positions (on/off), and can be connected with timers for delayed on/off, a display of all current device activities, such as start of scanning, success of process, results of generating unique ID reference generated during the process of fingerprint scanning, a button that starts the scanning process, reset button that resets acquired and processed data after storing it, a command button that saves and stores the data after scanning process and two fields for fingerprint scanning.

After starting the device with a P button, it performs a self-check and provides the user with an information on the display if it operates regularly and if there are no errors. By pressing the S button the fingerprint scanning on both fields of the device (S1 and S2) start simultaneously. After scanning and pressing R1 button the data will be stored and unique ID reference is shown on display D.

A cross-section of the device is shown on Fig. 2. The device may include the power supply (P), a wireless transmitter (W) that enables the device to transfer the encrypted data through a wireless communication channel to the server or communicate with other devices for biometric identification of maternity. The device may also use batteries (1.5V AA or AAA) placed in the slot B if a power supply is unavailable, due to a power outage, for example.

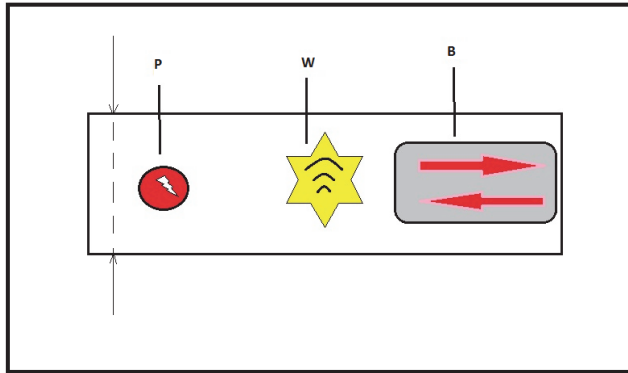


Fig. 2 – *Cross-section of the device.*

The communication between server and devices for biometric verification of maternity is presented on Fig. 3. Wireless communication may be provided with a wide range of various possibilities [18, 19].

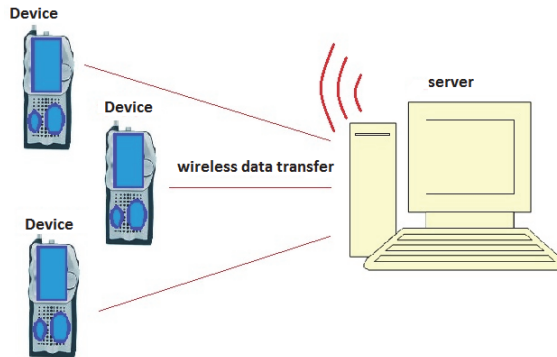


Fig. 3 – *Possible communication between server and devices.*

Various possibilities of storing and saving data received during fingerprint scanning process are presented on Fig. 4. Memory that is used is both RAM (Random Access Memory) and ROM (Read Only Memory), depending on the purpose of use Device provides all nowadays popular and common storage devices such as Memory card, EPROM (Erasable Programmable ROM), EEPROM (Electrically Erasable Programmable ROM) and Hard Disk.

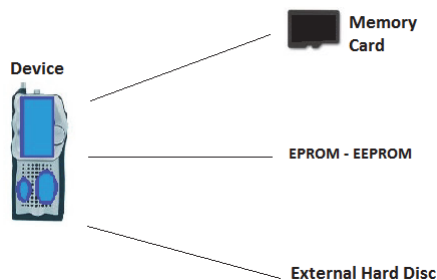


Fig. 4 – Possible data storage solutions.

Minutiae extracted from mother and child's scanned fingerprints and generated unique ID reference bounded to the pair is presented on Fig. 5.

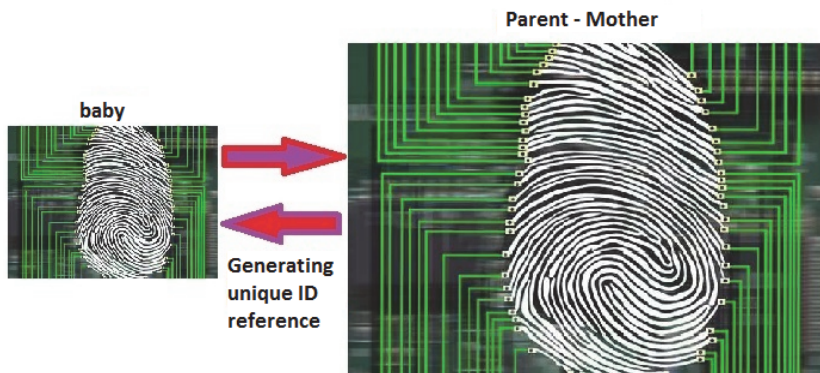


Fig. 5 – Mother and the baby's minutiae fingerprint scanned.

It is important to mention that after received information about the values acquired during the scanning process, the device software takes the result of the scanned fingerprint minutiae and ID reference and executes both mathematical and logical operations with the received data. As a result of those operations, the device produces check value over final data.

7 Conclusion

The device can be applied in dozen countries in a fight against the organized crime and help prevent thefts or replacements of newborn babies, especially in territories with low IT infrastructure and technological development. It is modular, it can be updated and what is most important, it can be a base for some future development in the area of biometric systems. Each biometric system tries to minimize verification error rates; this device has

accomplished that part since it combines two scanned samples and its accuracy grows exponentially.

Device is open for future implementation of hash functions over stored data that would improve data integrity. Hash values can provide advanced data check of the existing data as an additional control element. It is necessary to mention that results accepted during scanning process, with personal data, are encrypted before they are stored and saved in the device or a server, thus minimizing the possibility of compromising data [20]. This device with its essential idea about biometric verification of maternity can find place in further developments of similar biometry systems in day-care centers and in kindergartens where various problems exist regarding keeping an eye on small children in every moment. Also, it can be a part of a much larger Health Care system regarding small children in pediatric institutions, where the device can provide basic data about possible allergies of each child and can improve that part of health care system globally.

8 Acknowledgements

Authors would like to everybody who have supported this research: Lisa magazine, Ilustrovana politika, ALO magazine, RTS – Beogradska hronika, RTV Prva, RTV Pink, TN N1, Kopernikus, YU EKO RTV Subotica. A special gratitude goes to people that work at the Institute for Intellectual Property of the Republic of Serbia, MA/MSc Saša Zdravković. Komlen Lalović exclusive gratitude goes to his dear pregnant woman Jelena Lalović and baby Stefan.

9 References

- [1] <http://www.epo.org/index.html>.
- [2] NIST, A Survey of Access Control Methods.
- [3] M. Elgendi: On the Analysis of Fingertip Photoplethysmogram Signals, *Current Cardiology Reviews*, Vol. 8, No. 1, Feb. 2012, pp. 14 – 25.
- [4] <http://www.zis.gov.rs/pocetna.1.html>.
- [5] K. Kaplan-Sandquist, M.A. LeBeau, M.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, Feb. 2014, pp. 68 – 77.
- [6] S. Ferguson, L. Nicholson, K. Farrugia, D. Bremner, D. Gentles: A Preliminary Investigation into the Acquisition of Fingerprints on Food, *Science and Justice*, Vol. 53, No. 1, March 2013, pp. 67 – 72.
- [7] <http://neurotechnology.com>.
- [8] C. Moujahdi, G. Bebis, S. Ghouzali, M. Rziza: Fingerprint Shell: Secure Representation of Fingerprint Template, *Pattern Recognition Letters*, Vol. 45, Aug. 2014, pp. 189 – 196.
- [9] C. Lee, H.S. Shin, J. Park, J.H. Lee: The Optimal Attachment Position for a Fingertip Photoplethysmographic Sensor with Low DC, *IEEE Sensors Journal*, Vol. 12, No. 5, May 2012, pp. 1253 – 1254.

- [10] A.K. Jain, P. Flynn, A.A. Ross: Handbook of Biometrics, Springer Science and Business Media, NY, USA, 2007.
- [11] K. Moore, T.V.N. Persaud, M. Torchia: Before We Are Born: Essentials of Embryology and Birth Defects, Elsevier, London, UK, 2014.
- [12] NIST Publishes Compression Guidance for Fingerprint, Journal Elsevier – Biometric Technology Today, Vol. 2014, No. 4, April 2014, p. 12.
- [13] G. Schoenwolf, S. Bleyl, P. Brauer, P. Francis-West: Larsen's Human Embryology, Elsevier and Churchill Livingstone, Philadelphia, PA, USA, 2014.
- [14] A. Grzybowski, K. Pietrzak: Jan Evangelista Purkyně (1787–1869): First to Describe Fingerprints, Clinics in Dermatology, Vol. 33, No. 1, Jan/Feb. 2015, pp. 117 – 121.
- [15] E. Gutierrez-Redomero, N. Rivalderia, C. Alonso-Rodriguez, A. Sanchez-Andres: Assessment of the Methodology for Estimating Ridge Density in Fingerprints and Its Forensic Application, Science and Justice, Vol. 54, No. 3, May 2014, pp. 199 – 207.
- [16] H.G. Dahlen, S. Caplice: What Do Midwives Fear?, Women and Birth, Vol. 27, No. 4, Dec. 2014, pp. 266 – 270.
- [17] A.R. Kavsaoglu, K. Polat, M.R. Bozkurt: A Novel Feature Ranking Algorithm for Biometric Recognition with PPG Signals, Computers in Biology and Medicine, Vol. 49, June 2014, pp. 1 – 14.
- [18] A. Motamedi, M.M. Soltani, A. Hammad: Localization of RFID-equipped Assets During the Operation Phase of Facilities-Original Research Article, Advanced Engineering Informatics, Vol. 27, No. 4, Oct. 2013, pp. 566 – 579.
- [19] H. Cai, A. R. Andoh, X. Su, S. Li: A Boundary Condition based Algorithm for Locating Construction Site Objects using RFID and GPS, Advanced Engineering Informatics, Vol. 28, No. 4, Oct. 2014, pp. 455 – 468.
- [20] W.J.C. Verhagen, B. de Vrugt, J. Schut, R. Curran: A Method for Identification of Automation Potential through Modelling of Engineering Processes and Quantification of Information Waste, Advanced Engineering Informatics, Vol. 29, No. 3, Aug. 2015, pp. 307 – 321.