Biometric Verification of Maternity and Identity Switch Prevention in Maternity Wards

Komlen Lalović[1], Nemanja Maček[2], Milan Milosavljević[3], Mladen Veinović[4], Igor Franc[5], Jelena Lalović[6], Ivan Tot[7]

[1,3,4] Faculty of Informatics and Computing, Singidunum University, 32 Danijelova Street, 11000 Beograd, Serbia; e-mails: komlen.lalovic.13@singimail.com, mmilosavljevic@singidunum.ac.rs, mveinovic@singidunum.ac.rs

[2,5] SECIT Security Consulting, 21/3 Aksentija Maksimovića Street, Pančevo, Serbia; e-mail: nmacek@secitsecurity.com, ifranc@secitsecurity.com

[6] Golden Mind Ltd, 11 Pohorska Street, 11070 Novi Beograd, Serbia,
e-mail: office@GoldenMind.rs

[7] Military Academy, 33 Pavla Jurišića Šturma Street, 11000 Beograd, Serbia,
e-mail: ivan.tot@va.mod.gov.rs

Abstract: This paper presents a novel approach to noninvasive biometric maternity verification and baby-switching prevention in maternity wards based on dual biometric fingerprint scanner. The proposed system is expected to solve issues that have occurred in many countries regarding stealing or mixing the identities of newborn babies. The solution is based on a device that acquires biometric samples from the mother and her newborn baby right after birth and generates the unique reference of the pair. The same device is used to verify the bound of biometric samples before the mother and the baby are allowed to leave the maternity ward. The privacy of stored templates is provided by cancelable biometrics while the auxiliary data are secured with strong cryptographic protection. The main contribution of the proposed approach is a very high level of proof of maternity for each newborn baby, as well as, the prevention of replacing identities of newborn babies in maternity wards, with a system that can be realized via low cost hardware.

Keywords: biometrics; fingerprint; minutiae; maternity; identity

1 Introduction

Babies switched in maternity hospitals are babies who are interchanged with each other at birth and raised by non-biological parents. According to Brandon Gaille, about 28,000 babies out of 4 million total births are switched every year [1]. Although Gaille stated that many of these cases are solved at some point before families leave the hospital, the objective risks of switching babies still exist and these issues need to be resolved. The major cause behind baby-switching is human error. As an example, officials of Smith N. Mercy hospital stated definitively, that human error was the reason for such a mistake [2]. Once an incident is discovered, lawsuits against hospitals may occur. Two mothers whose infant sons were switched by medical personnel at Heartland Regional Medical Center brought a lawsuit against the hospital [3]. The switching of two Russian newborn girls was discovered after the ex-husband of one of the mothers had refused to pay alimony on the basis that she looked nothing like him and requested a DNA test [4]. Both families raised a lawsuit against the hospital. Crane provided a more detailed analysis on hospital liability and resulting custody issues [5]. Another aspect that should also be seriously considered is the maternity patient's levels of anxiety. Davis et al. stated that media reports in the USA of baby-switching caused anxiety of a number of patients, and, according to an experimental study, 10% of the mothers reported anxiety about baby-switching [6]. According to Rusting, baby-switching is a problem that can have the same impact on a healthcare facility as an infant kidnapping [7]. The fears of maternity health providers, including. but not limited to baby-switching, and the impact on the women they care for are discussed by Dahlen and Caplice [8]. Although some hospitals implement certain precautionary procedures, no 100% proof of maternity verification technique has been reported in the literature.

This paper presents a maternity verification approach based on fingerprint biometric trait matching. Biometric verification is the process of validating the identity of individuals according to their physiological or behavioral qualities [9], [10]. A fingerprint is the only physiological quality that is completely formed during the prenatal period [11]. By the end of the 7th month of pregnancy, minutae point structure on each finger of the fetus is formed and the ridge shape remains constant during their entire life. Prenatally formed shape of fingerprint ridges and valleys allows biometric template acquisition of a newborn baby that can later be used for maternity verification, even if the baby is born premature, e.g. in the 8th month of pregnancy [12]. Unlike fingerprint, the other physiological traits are unstable at birth. For example, the pigmentation of child’s eye is changes until the age of four [13], resulting in an unstable iris acquisition and verification process for newborn babies. That is why the proposed approach employs the fingerprint biometrics. Biometric traits of a baby and the mother are acquired right after the birth on a dual fingerprint scanner; the unique reference is generated and the data is stored in a secure manner on the device. At any time, the identity of the mother and the baby can be verified on the same device, e.g., before breast-feeding. Before leaving the maternity hospital a final verification is performed, and the data are securely wiped from the device. The proposed approach employs cancelable biometrics to provide the privacy of stored templates and cryptography to provide security of stored auxiliary data.

2 Dual Fingerprint Scanner

Device for biometric identification of maternity [14] is dual fingerprint scanner, registered patent number 1412 U1 at the Institute of Intelectual Property, Republic of Serbia. It won the Belgrade City Award for the best Patent Innovation in the field of natural sciences in 2014. According to the International classification of patents, this patent is classified with a symbol G06F21/00, as it belongs to the biometric systems – fingerprint scanning devices. Fingerprint scanners use different algorithms and methods to authenticate or verify the identity of individuals. However, no device has been found in the National Database of Patents [15] that operates as dual fingerprint scanner or a fingerprint scanner capable of providing any kind of match between two persons. An example of single fingerprint scanner can be found in the patent confirmation 13848069.4, issued on April 2, 2013, with remark WO2014059761 and classification G06F21/00 ("Fingerprint identification device"). The device used in this research employs two optical sensors that simultaneously acquire biometric samples of two different persons. Once the acquisition of samples is complete in the enrollment phase, the device extracts features, generates cancelable biometric templates and unique ID reference that bonds those templates. Generated reference and cancelable templates are stored on the device in a secured manner. During the verification phase, the stored reference is used as an undeniable proof of identity match of two persons that provided their samples in enrollment phase.

2.1 Detailed Device Description

The device for biometric identification of maternity, contains the following components:

- Ignition switch that can be connected with delay timer (I),
- Display that can provide information on all current activities and results of generating unique ID reference,
- Start button (S1) that starts the fingerprint scanning,
- Store button (S2) that secures and stores the data after scanning,
- Reset button (R) that resets acquired and processed data, after storing it,
- Numerical keyboard that is used to acquire PIN,
- Two fingerprint scanning sensors (S1 and S2) for a mother and the baby. Larger sensor is used to scan mother's finger with 500 dpi resolution. Smaller sensor scans the baby's finger with at least 1000 dpi resolution as the ridge structure image is harder to acquire due to the size of the finger [16].

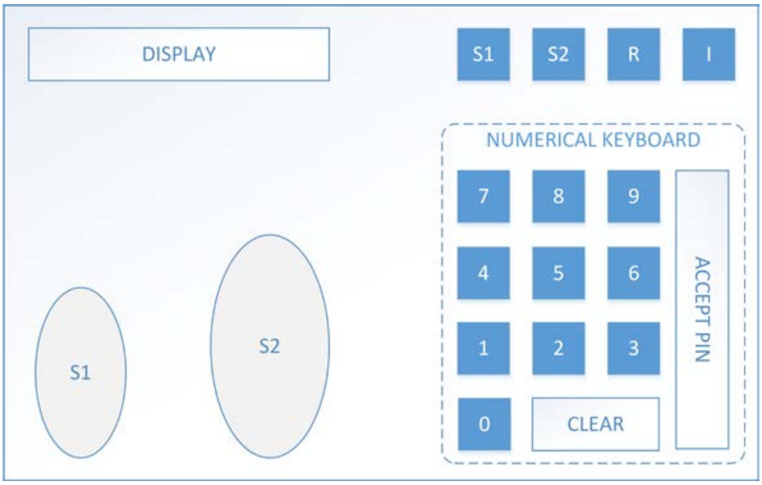

Figure 1
Device for biometric identification of maternity

The device operates as follows: the device started via ignition switch performs a self-check and provides the user with the information if it functions properly or not. After the start button is pressed, the device requires mother's and baby's fingers to be placed on sensors and starts scanning their fingerprints simultaneously. After the scanning, the unique ID reference is generated. Mother enters a PIN code on the numerical keyboard and accepts it. Once the store button is pressed, the data is secured and stored in the memory of the device, as described in chapters 3 and 4 of this paper.

The device employs memory cards for storing the acquired data. It should be stated that the device is still in the development phase and that additional functionalities, such as storing the data on a remote server via encrypted wireless communication channel, will be added subsequentially.

3 Proposed Maternity Verification Algorithm

The main idea behind our approach is to employ simultaneous dual fingerpint scanning, cancelable biometrics and cryptographic protection of the auxiliary data. The proposed approach that employs noninvasive biometrics is expected to provide 100% proof of maternity verification, template privacy and stored data security.

During the enrollment phase, the system operates as it is shown in Figure 2.

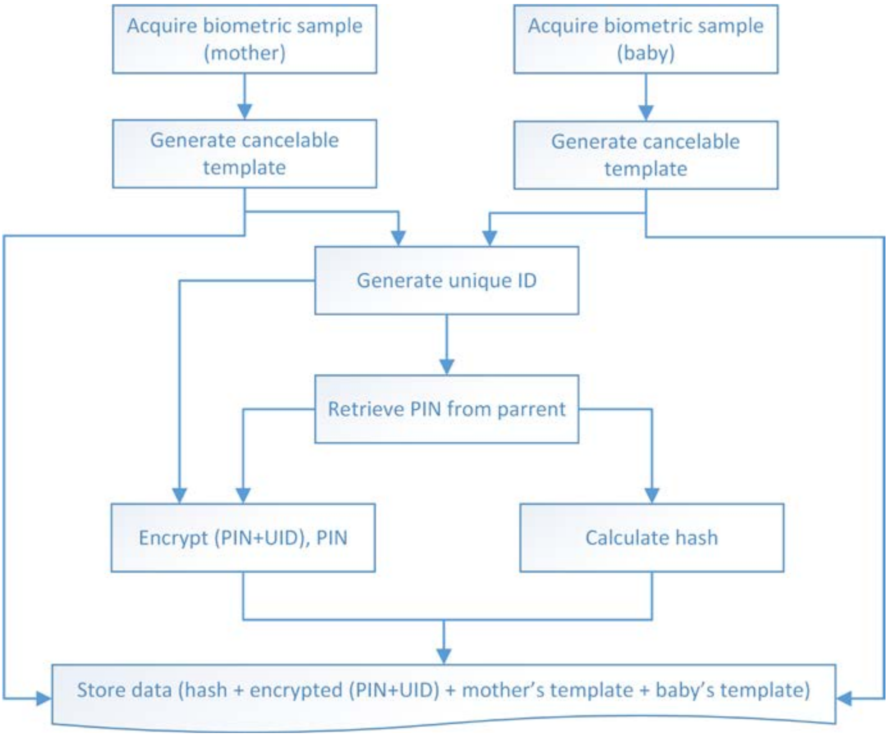
Acquire biometric sample (mother)
Acquire biometric sample (baby)
Generate cancelable template
Generate cancelable template
Generate unique ID
Retrieve PIN from parrent
Encrypt (PIN+UID), PIN
Calculate hash
Store data (hash + encrypted (PIN+UID) + mother's template + baby's template)

Figure 2
Enrollment phase

1) Biometric data from a mother and the baby are acquired by the sensor simultaneously. If the scan is unsuccessful, the scanning is repeated.
2) Data is preprocessed and both cancelable biometric templates are generated with non-invertible transforms.
3) Unique ID reference (UID) is generated.
4) Mother enters a 6-digit long PIN code on the the numerical keyboard and accepts it.
5) Unique ID is concatenated to and encrypted with provided PIN using symmetric encryption.
6) Hash of the PIN code is calculated.
7) A record is added to database containing the calculated hash of the PIN, the encrypted concatenation of UID and PIN, and both cancelable templates. The entire record may additionally be encrypted with a system-wide key (this functionality will be added subsequentially).

During the verification phase, the system operates as it is shown in Figure 3.

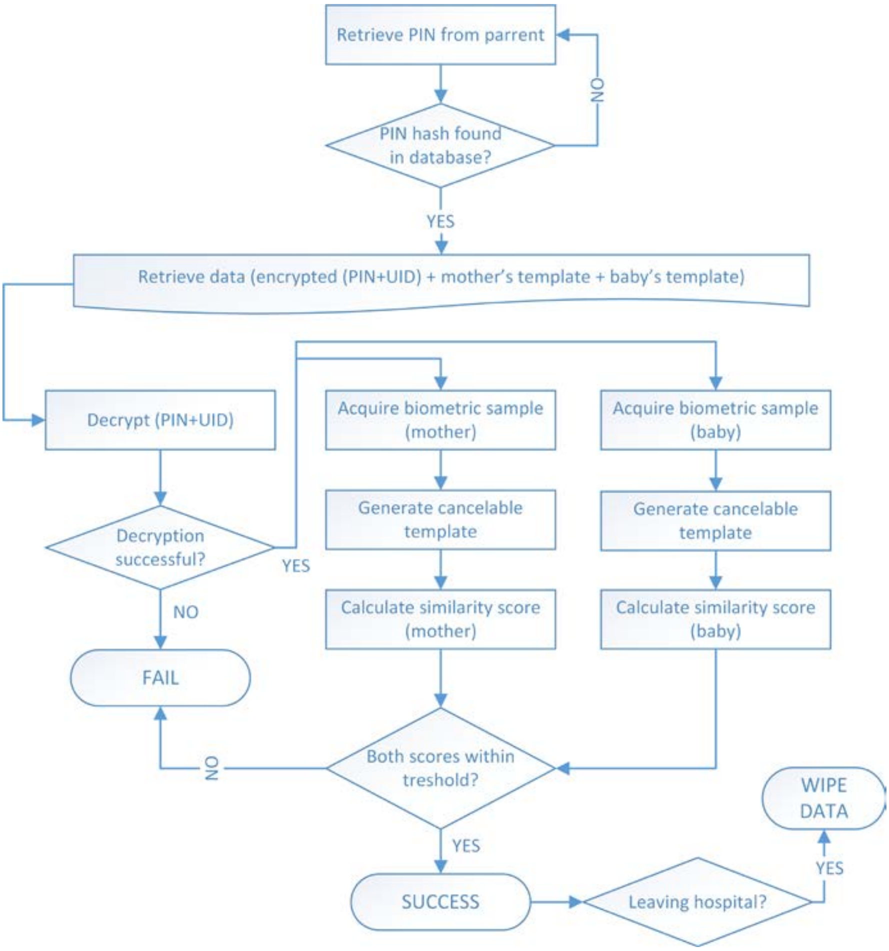
Retrieve PIN from parrent
PIN hash found in database?
NO
YES
Retrieve data (encrypted (PIN+UID) + mother's template + baby's template)
Decrypt (PIN+UID)
Decryption successful?
YES
NO
FAIL
Acquire biometric sample (mother)
Generate cancelable template
Calculate similarity score (mother)
Acquire biometric sample (baby)
Generate cancelable template
Calculate similarity score (baby)
Both scores within treshold?
NO
YES
SUCCESS
Leaving hospital?
YES
WIPE DATA

Figure 3
Verification phase

1) The mother is asked to provide a PIN code.

2) Hash of provided PIN is calculated. If no corresponding hash is found in the database, the mother is asked to retry.

3) If the corresponding hash is found, PIN is used to decrypt the stored cyphertext. If the PIN retrieved from the decrypted cyphertext matches the provided one, decryption is considered to be successful and the device continues to operate. If the decryption fails, device stops.

4) Biometric data from the mother and the baby are acquired by the sensor simultaneously. If the scan is unsuccessful, the scanning is repeated.

5) Data are preprocessed and both cancelable biometric templates are generated with non-invertible transforms.

6) Generated templates are compared with the ones stored in the database using cancelable biometrics. The verification is considered successful only if the similarity scores calculated between generated cancelable biometric templates and the one stored in the database are above predefined threshold, both for the mother and the baby.

7) If the verification is final (mother is leaving the maternity hospital with her baby) the data are securely wiped from the database.

4 Biometric Template Generation and Verification

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip [17], the formation of which is determined during the first seven months of fetal development [10]. Fingerprint ridges are noncontinuous lines. Ridges end and form ridge termination points, or split and form bifurcation points [17]. These points are called minutiae points and they are used as features in fingerprint recognition systems. According to Jain et al., the accuracy of the currently available fingerprint recognition systems is adequate for verification systems and medium-scale identification systems [10].

This research adopts the minutiae extraction method presented by Jagadeesan and Duraiswamy [18]. Details on the minutiae extraction can also be found in [19]. The process involves image preprocessing, segmentation, orientation field estimation, image enhancement and minutiae extraction. The first operation applied to the image in the preprocessing phase is histogram equalization that increases the local contrast of the image, resulting in overall contrast improvement. Wiener filter [20] removes blur and additive noise from the picture without altering ridge structures. Filtered image is further segmented and regions of interest are separated from the rest of the image. Let N denote the size of the block and $\mu(I)$ the mean pixel value of the block. Block I is considered to be foreground block if its variance is greater than the threshold τ_s:

$$\sigma^2(I) = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(I(i,j)-\mu(I)\right)^2 > \tau_s . \qquad (1)$$

The local orientation of ridge valley structures is further estimated. This operation is also a block-wise operation and it employs gradient vectors that indicate the highest deviation of gray intensity normal to the edge of ridge lines [21]. The resulting image is enhanced by Gaussian low-pass filter followed by the 2-D Gabor filter. Let f_0 denote ridge frequency, θ the orientation of the filter, σ_x and σ_y standard deviations of the Gaussian envelope along x and y axes, and $[x_\theta, y_\theta]$

coordinates of [*x*, *y*] after clockwise rotation of the Cartesian axes by 0.5*π*–*θ*. The 2-D Gabor filter is given by:

$$G\left(x, y, \theta, f_0\right) = \exp - \frac{1}{2}\left(\frac{x_\theta^{\ 2}}{\sigma_x^{\ 2}} + \frac{y_\theta^{\ 2}}{\sigma_y^{\ 2}}\right)\cos(2\pi f_0 x_\theta), \tag{2}$$

$$x_\theta = x\sin\theta + y\cos\theta, \tag{3}$$

$$y_\theta = -x\cos\theta + y\sin\theta. \tag{4}$$

The output if 2-D Gabor filter is binarized, resulting in the image with two levels of interest: ridges (black) and valleys (white pixels). Morphological operators are applied in order to eliminate the noise resulting from spurs and line breaks, followed by thinning algorithm presented by Lam et al. [22] that reduces the width of ridge lines. The thinning algorithm segments the image into two subfields as in the checkboard pattern, employs Hilditch crossing number and defines four pixel removal conditions that are used in the iterations of the algorithm. The result of the algorithm is the image composed of one pixel wide ridges, with clearly visible minutiae, as shown in Figure 4.

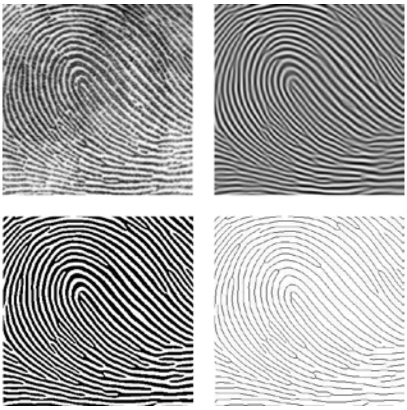

Figure 4
Original image (top left), enhanced image (top right), binarized image (bottom left) and thinned image (bottom right)

Let $p_1, p_2, \ldots p_8 \in [0, 1]$ denote neighbor pixels of pixel *p*, starting from the one on the right and counting counter clockwise. Crossing number $X_R(p)$ is calculated for each pixel in the resulting image, as the number of transitions from white to black and vice versa when points are traversed in order:

$$X_R\left(p\right) = \sum_{i=1}^{8}\left|p_{i+1} - p_i\right|. \tag{5}$$

Pixel *p* is identified as ridge termination point if $X_R(p) = 2$, and valley termination point (bifurcation) if $X_R(p) = 6$.

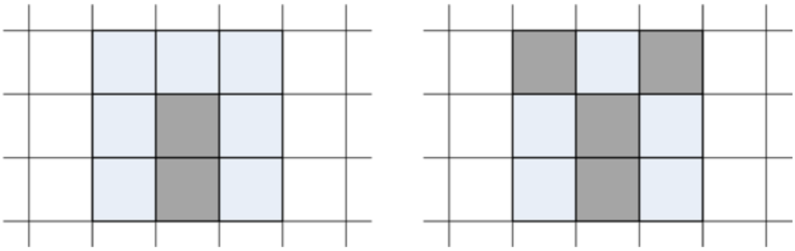

Figure 5
Termination point (centered pixel on the left) and bifurcation point (centered pixel on the right)

Fingerprint template is given by two-dimensional vector that contains cartesian coordinates of *n* extracted minutiae points:

$$F = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\} . \tag{6}$$

Non-invertible transforms are applied to extracted feature vector to preserve privacy of stored biometric data. According to Ratha et al., the transformation is invertible if the minutiae positions after transformation are highly correlated to minutiae positions before transformation [23]. Having that said, the goal of the transform is to eliminate minutiae correlation to the maximum possible extent and provide tolerance to brute force attacks.

This research employs minutia shuffling transform that depends on the PIN. The transform proposed by authors operates as follows. The coordinate system is divided into 4 x 4 cells. Each minutiae is clockwise relocated from one cell to another depending on the one digit of PIN, while the relative position from top-left corners of the originating and destination cells remains unchanged (as shown in Figure 6). The transformation starts with the first PIN digit and top left minutiae and ends up with the one at the bottom right. Each seventh minutiae is transformed using the first PIN digit. The transform is non-invertible as is impossible to determine the original cell of the minutiae. More details on security of cancelable fingerprint templates can be found in [24]. The impact of the transform on matching accuracy is discussed in Section 5 of this paper.

Generated cancelable template consists of shuffled minutia point coordinates. Templates are generated both for the mother’s and the baby’s fingerprints and stored on the device alongside encrypted UID and hash of the PIN.

During the verification phase, the same procedure is performed and another vector is generated. Missing points are discarded, the sum of the squared differences between two feature vectors is calculated, normalized by the number of remaining non-discarded values, and the matching score is compared with a threshold.

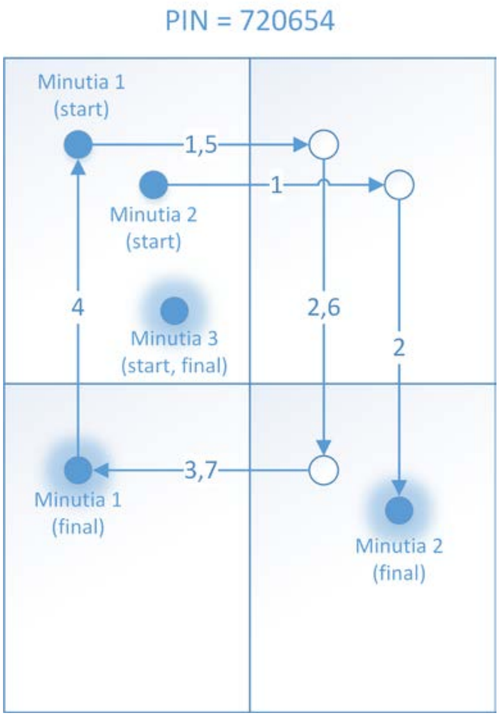

Figure 6
PIN-dependent non-invertible transform

5 Experimental Evaluation

Two sets of experiments were conducted to evaluate the proposed solution. First, experiments that provide a proof that scanning baby's fingerprints is possible were conducted. The type of sensor that provides lowest Failure to Enroll rates and high verification performance were also identified. These experiments were run with prior written permission from parents. Due to legal and ethical aspects of children fingerprint acquisition for the purpose of experimentation, images from CASIA-FingerprintV5 [25], collected by the Chinese Academy of Sciences' Institute of Automation, were used as inputs in the second set of experiments. The second set of experiments evaluates the performance of the proposed system.

5.1 Baby's Fingerprints and Commercial Scanners

In the first set of experiments, the fingerprints of a 3 month old child were acquired with three different types of commercial scanners: optical, thermal and capacitive. Optical scanners take an image of the fingerprint using a camera. The device used in this experiment is Futronic FS80H USB 2.0 scanner. Capacitive scanners use capacitors to form an image of the fingerprint from electrical current. The device used in this experiment is Eikon II Swipe. Thermal scanners sense the temperature differences on the contact surface, between fingerprint ridges and valleys. The device used in this experiment is id3 Semiconductors Certis Image that employs Atmel FingerChip thermal sensor. More information on these devices is available on Fulcrum Biometrics [26]. In this experiment, ten attempts were made to acquire a biometric template of each finger of the right hand. Acquisition results and Failure to Enroll rates (FTE) are given in Table 1.

Table 1
Baby's fingerprint FTE on optical, capacitive and thermal scanner

	Sensor type		
Finger	**Opical**	**Capacitive**	**Thermal**
Thumb	10	7	2
Index finger	10	7	2
Middle finger	10	6	1
Ring finger	10	5	0
Pinky	9	4	0
% successful	98%	56%	10%
Failure to Enroll (%)	2%	44%	90%

According to the results given in Table 1, it can be concluded that the optical scanner outperforms both capacitive and thermal ones. The optical scanner failed to enroll only the pinky finger once, due to smaller size of ridge structures. Due to acceptable 2% Failuire to Enroll rate, the optical scanner is further used to evaluate the success of identity verification. The templates of each finger are created and stored, and each finger is further verified against 10 reacquired biometric samples. The optical scanner failed to verify both ring finger and pinky twice, which results in 4% False Rejection Rate (FRR).

5.2 Experimental Evaluation of the Proposed System

The Performance of the proposed solution is experimentally evaluated using MATLAB R2015a (feature extraction) and Python 2.7 (matching, cancelable template generation and scripting). We have conducted our experiments as follows. CASIA database contains five images of each finger for 500 subjects. A set containing 10 pairs of index finger images was created and used to enroll genuine users. One image in each pair represents the mother and the other represents the child. Each pair was associated with UUID and randomly generated 6-digit PIN during the enrollment phase. The accuracy of the system was measured by verifying each pair of fingerprints with: 10 pairs that contain remaining images belonging to those people (images not used to enroll users), 5 pairs that contain genuine image of one person and an imposter image for the other person and 5 pairs that contain both images belonging to imposters. Matching scores have been scaled to range [0, 1] and compared with several threshold values. The verification is considered to be successful if matching scores for both fingers in the pair are above the threshold. The definition of False Acceptance Rate (FAR) and False Rejection Rate (FRR) is slightly altered as the system verifies two fingerprints at the same time. False acceptance in this scenario occurs if the system identifies at least one imposter fingerprint in the pair as genuine user during the verification. False rejection in this scenario occurs if the system identifies at least one genuine fingerprint in the pair as imposter. Experiments were conducted with the aim to evaluate the overall accuracy of the fingerprint matcher, the impact of cancelable biometric template protection and overall security of the system.

First the fingerprint matcher that does not involve cancelable biometric templates and PIN protection was tested. The results of the experiments are given in Table 2 and graphically presented on Fig. 7.

Table 2

Verification summary of the dual fingerprint matcher for different treshold values

Verification matrix			**Treshold**					
Input pair	#	**Identified as**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**
Both genuine	100	Genuine	96	97	99	99	100	100
		Imposter	4	3	1	1	0	0
Genuine and imposter	50	Genuine	1	1	2	2	5	7
		Imposter	49	49	48	48	45	43
Both imposter	50	Genuine	0	1	1	1	4	5
		Imposter	50	49	49	49	46	45
False rejection rate (%)			4%	3%	1%	1%	0%	0%
False acceptance rate (%)			1%	2%	3%	3%	9%	12%

Experimentally obtained results given in Table 2 were not surprising as false rejection rate decreases and false acceptance rate increases with the threshold being loosen up (see Fig. 7).

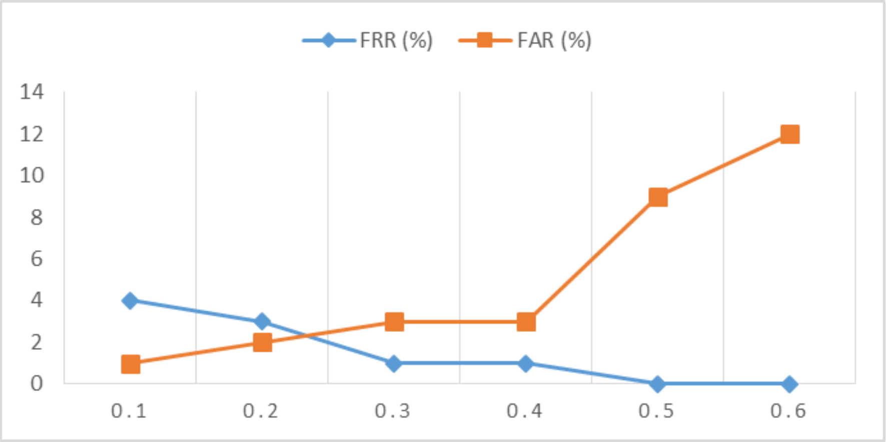

Figure 7

FAR and FRR of the dual fingerprint matcher

The second set of experiments introduces cancelable biometrics to the system. The results of the fingerprint matcher that employs cancelable biometric template generation algorithm proposed by authors are given in Table 3.

Table 3

Verification summary of the dual fingerprint matcher that employs cancelable biometric templates for different threshold values

Verification matrix			Treshold					
Input pair	**#**	**Identified as**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**
Both genuine	100	Genuine	93	94	96	98	99	100
		Imposter	7	6	4	2	1	0
Genuine and imposter	50	Genuine	1	2	2	3	7	9
		Imposter	49	48	48	47	43	41
Both imposter	50	Genuine	1	1	1	2	6	6
		Imposter	49	49	49	48	44	44
False rejection rate (%)			7%	6%	4%	2%	1%	0%
False acceptance rate (%)			2%	3%	3%	5%	13%	15%

As we have expected, the non-invertible transform has introduced additional errors to the matcher. FRR is increased for lower threshold values, while FAR increases to the unacceptable level for loosen thresholds. Optimal threshold for this system is found via equal error rate (EER), as presented on Fig. 8.

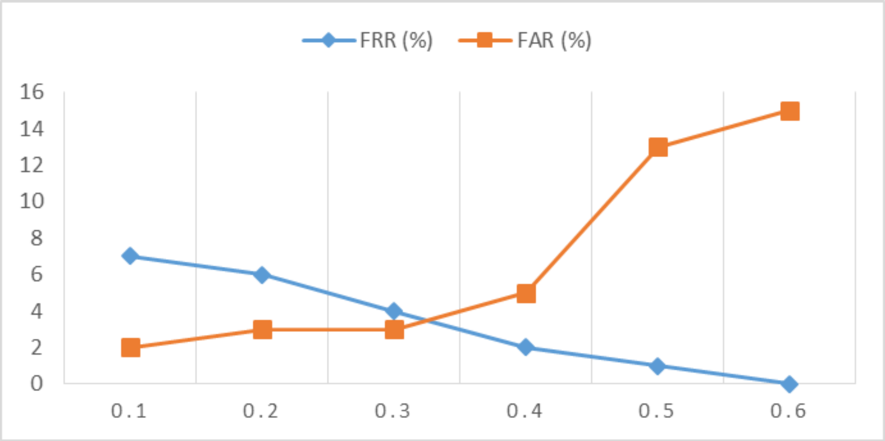

Figure 8
FAR and FRR of the dual fingerprint matcher that employs cancelable biometric templates

Threshold value t = 0.325 results with an 3.5% EER. This error is slightly higher when compared to a system that does not employ cancelable templates: 2.3% EER occurs on threshold value t = 0.23. Having in mind that cancelable biometrics protects the privacy of stored templates and prevents possible malicious misuses, this small increasing of EER is further treated as negligible.

Once optimal EER is determined, the PIN and cryptographic protection are further introduced to the system. Minutiae points were extracted from the set of CASIA fingerprint images and Python scripts were run to simulate the enrollment and verification phases of the entire system, as presented on Fig. 2 and Fig. 3. PINs were generated randomly during the enrollment and stored in a sepatate file, as they are required for the verification. With the exception of the PIN being stolen or compromised in any other way, it can easily be concluded that the cryptographic protection eliminates any chance of false accepts occuring. 3.25% False Rejection Rate results with one reject in approximately 30 attempts, which is an acceptable result for intended application as users are allowed to repeat the verification step if it fails.

5.3 Discussion

As stated in the section 3 of the paper, the main goal was to reach a very high level of proof of maternity using noninvasive biometrics and provide the sufficient level of security with cancelable biometrics (non-invertible transforms). Although no dual fingerprint scanners are found in National Database of Patents, the Republic of Serbia [15], some commercial solutions do exist on the market, such as [27]. By conducting a detailed background research, these are used to enroll or verify the identity of one person using two different fingers, thus reassembling single trait – multiple units scenario in multimodal biometric system classification of Ross and Jain [28]. Our approach to dual fingerprint scanning is different and unique: it generates cancelable templates from two fingers belonging to different people and makes a bond between them, thus finding an application in maternity verification and identity theft prevention in maternity wards.

The performance and security of the proposed solution, as well as some ethical aspects behind the application of the device are further discussed. We have identified the performance of the system as satisfactory: according to the experimental evaluation, system rejects 3.5% genuine users. However, users are allowed to retry and therefore this does not set an obstacle to keeping the high level of security by employing tight threshold and non-invertible transform. The cryptographic protection of auxiliary data eliminates the chance of false acceptance as only the users who know the PIN can proceed to the verification. The security of the system depends on several factors, and an adversary who wants to steal the baby, for example, would have to override the auxiliary data encryption and non-invertible tranform. Some may set up ethical obstacles to the application of this device by asking the following question: “can the biometric templates be misused?” The answer is no. Even if the PIN is known, it is impossible to regenerate original templates from cancelable ones using anything other than brute force. A brute force attack on 4x4 cell shuffler would require in $(4x4)^{(4x4)}$ attempts, which is approximately 18.5 x 10^{18} attempts. And all the data are securely deleted from the storage once the mother and the child leave the hospital.

By conducting informal inquiries, one critical issue in the whole approach was identified: the problem of forgetting PIN codes. Mother is emotionally driven at the time of birth and a reasonable chance exists for her to forget the PIN she has entered right after birth. Authors are discussing several methods that will provide recovery of the data, such as some key escrow techniques.

Conclusions

Although various anti baby-switching procedures are implemented in hospitals world wide, no 100% proof maternity verification method is reported in the literature or, to the best of our knowledge, used in any maternity wards. The major contribution of the approach presented in this paper based on a patented dual fingerprint scanner is the elimination of anxiety caused by baby-switching and the provision of a proof to each mother that she will leave the maternity hospital with her own child. Additionally, each mother may require biometric verification of her baby during breast-feeding, for example. The proposed approach also removes the possibility of subsequent lawsuits and traumas resulting from baby-switching. As the device stores the templates processed with PIN-dependent non-invertible transforms and securely wipes them when the family leaves the maternity hospital, the concern about biometric template privacy or identity theft is also eliminated. As an average a high-quality fingerpint scanner costs no more that \$100-\$150 and the algorithms presented in this paper can be easily implemented on a low-cost hardware, it is expected that this device will be affordable for each hospital.

References

[1] B. Gaille: 20 Rare Babies Switched at Birth Statistics. Tips from the Blog Millionaire. July 29, 2014

[2] Williston Herald. November 11, 2009

[3] John D. Homan, TheSouthern.com, April 11, 2008

[4] Steve Rosenberg, BBC News, Moscow, October 10, 2011

[5] T. R. Crane: Mistaken Baby Switches: an Analysis of Hospital Liability and Resulting Custody Issues. Journal of Legal Medicine, 21(1), pp. 109-124, 2000

[6] J. D. Davis, M. K. Moran, E. O. Horger III, A. N. Dajani: Pregnancy Anxieties and Natural Recognition in Baby-Switching. British Journal of Nursing, 10(11), pp. 718-726, 2001

[7] R. R. Rusting: Baby Switching: an Underreported Problem that Needs to be Recognized. Journal of Healthcare Protection Management: Publication of the International Association for Hospital Security, 17(1), pp. 89-100, 1999

[8] H. G. Dahlen, S. Caplice: What do Midwives Fear?. Women and Birth, 27(4), pp. 266-270, 2014

[9] A. K. Jain, A. Ross: Introduction to Biometrics. In “Handbook of Biometrics”, A. Jain et al. (Eds), Springer, 2008

[10] A. K. Jain, A. Ross, S. Prabhakar: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, pp. 4-20, 2004

[11] K. Moore, T. V. N. Peraud, M. Torchia: Before We Are Born, 9th Edition. Elsevier UK, 2014

[12] G. Schoenwolf, S. Bleyl, P. Brauer, P. Francis-West: Larsen's Human Embryology, 5th Edition. Elsevier Health Sciences, Churchill Livingstone, 2014

[13] A. R. Kavsaoğlu, P. Kemal, M. R. Bozkurt: A Novel Feature Ranking Algorithm for Biometric Recognition with PPG Signals. Computers in Biology and Medicine 49, pp. 1-14, 2014

[14] K. Lalović, M. Milosavljević, I. Tot, N. Maček: Device for Biometric Verification of Maternity. Serbian Journal of Electrical Engineering, Vol. 12, No. 3, pp. 293-302, 2015

[15] http://www.zis.gov.rs/pocetna.1.html

[16] C. Lee, H. S. Shin, J. Park, M. Lee: The Optimal Attachment Position for a Fingertip Photoplethysmographic Sensor with Low DC. Sensors Journal, IEEE, 12(5), pp. 1253-1254, 2012

[17] T. Van der Putte, J. Keuning: Biometrical Fingerprint Recognition: don't Get Your Fingers Burned. In Smart Card Research and Advanced Applications (pp. 289-303) Springer US, 2000

[18] A. Jagadeesan, K. Duraiswamy: Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. International Journal of Computer Science and Information Security, Vol. 7, No. 2, pp. 28-37, 2010

[19] N. Maček, B. Đorđević, J. Gavrilović, K. Lalović: An Approach to Robust Biometric Key Generation System Design. Acta Polytechnica Hungarica, Vol. 12, No. 8, pp. 43-60, 2015

[20] H. Furuya, S. Eda, T. Shimamura: Image Restoration via Wiener Filtering in the Frequency Domain. WSEAS Transactions on Signal Processing, 5(2), pp. 63-73, 2009

[21] Y. Wang, J. Hu, F. Han: Enhanced Gradient-based Algorithm for the Estimation of Fingerprint Orientation Fields. Applied Mathematics and Computation, Special Issue on Intelligent Computing Theory and Methodology, Vol. 185, No. 2, pp. 823-833, 2007

[22] L. Lam, S. W. Lee, C. Y. Suen: Thinning Methodologies - a Comprehensive Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 14(9), pp. 869-885, 1992

[23] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle: Generating Cancelable Fingerprint Templates. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), pp. 561-572, 2007

[24] C. Li, J. Hu: Attacks via Record Multiplicity on Cancelable Biometrics Templates. Concurrency and Computation: Practice and Experience, 26(8), pp. 1593-1605, 2014

[25] Biometrics Ideal Test, http://biometrics.idealtest.org

[26] http://www.fulcrumbiometrics.com/

[27] http://www.m2sys.com/dual-fingerprint-biometrics/

[28] A. Ross, A. K. Jain: Multimodal Biometrics: An Overview. In Signal Processing Conference, 2004 12th European, pp. 1221-1224, 2004, IEEE