

# Comparing Physiological Similarities between Fingerprints of Family Members by MorphoSmart Finger VP Scanner

Hana Talandova, Hana Urbancokova and Milan Adamek

Faculty of Applied Informatics  
Tomas Bata University in Zlin  
nam. T.G.Masaryka 5555, 760 01 Zlin  
Czech Republic  
{talandova, urbančokova, adamek}@fai.utb.cz

**Abstract**— This paper discusses the use of the scanner MorphoSmart Finger VP for comparison of the similarity between fingerprints of family members. The paper is divided into four sections. The first two sections are focused on introducing the biometrics as a complex and then explain one of the most spread biometric identification method - fingerprints. The next section describes the use of a fingerprint scanner and determining its error rate. In the last part of the paper is described an experiment which compares the similarity of the fingerprints between family members with subsequent evaluation of these results.

**Keywords**— Scanner, biometry, biometric identification, fingerprints, experiment.

## I. INTRODUCTION

Biometrics is an advanced method for user identification based on the measurement of the provided biometric data. These data are used to grant or deny access to the object (buildings, databases ...). Biometric features can be divided into two groups - the physiological and behavioral (for example voice) (Fig. 1).

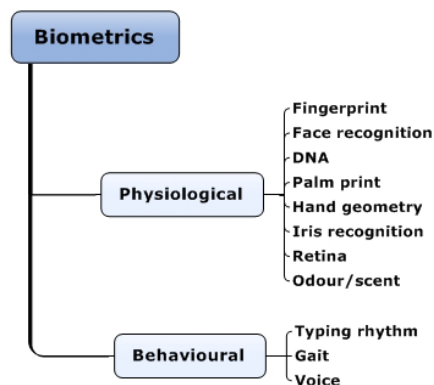


Fig. 1. Division of biometric features

Biometric system can be used for identification or verification. During the process of verification the identity of person is known and it is only verified on the basis of a specified data with entry in the database. This is a fast process which result is granted or denied access. In the process of identification, the identity of person is unknown. The system compares the identification data with other data stored in the database. On the basis of comparison (match is found) is granted or denied access. Verification of the persons may be supplemented by traditional methods such as PIN, magnetic cards, keys, etc. The distribution of user authentication options for access is on the Fig. 2.

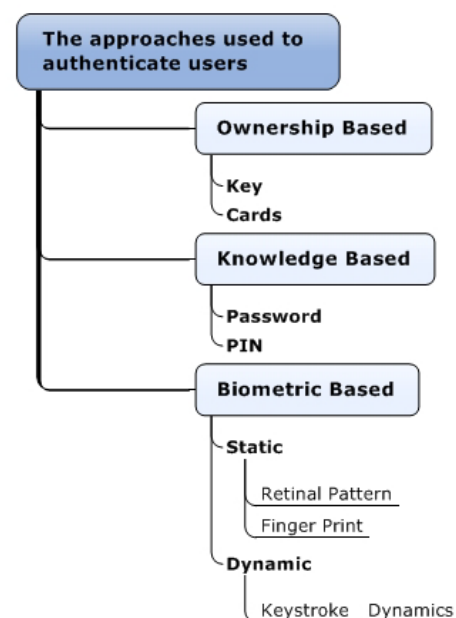


Fig. 2. Distribution of authentication user option

Biometric systems are introduced seventies. It is a system which recognizes newly captured biometric data whit already collected data, which is stored in the database. Then the system evaluates if it is an authorized person or not (grant or deny access). Biometric system works in three phases which are shown on Fig 3.

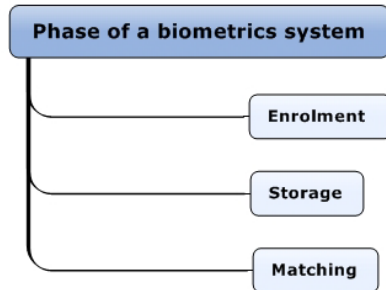


Fig. 3. Main phases of biometric system

In the first phase the biometric system collects biometric data from the user. These data are captured and then stored in a database. This process of writing required of all who will be allowed access to the object or the database. In the second phase are extracted unique characteristics of the scanned biometric data from the first phase. The last phase is the phase of verification and evaluation of access. At that moment, the newly captured biometric data of users are compared with the already stored data in database and then is evaluated if it is an authorized person or not (grant or deny access).

It has been designed many biometric systems based on recognition of biometric data which have to improve the security and user friendliness. Each of these systems has its own advantages and disadvantages. For retinal scanner causes an unpleasant feeling and fears about eye. For identification using hand geometry may be a problem with people with arthritis or the rheumatism and with fingerprint scanning is a problem with dirty. Therefore, new identification method was developed. This method is based on scanning of palm vein and it is solve problems which were described and of course it is much more user friendly.

## II. FINGERPRINTS

The fingerprints are probably the best known and most widely used of all the biometric technologies. The fingerprint is widely used in police-judicial sector and in security-commercial sector. Fingerprints in the police-judicial sector are used primarily for the identification of perpetrator of a crime who unintentionally left the fingerprints at the crime scene. In security-commercial sector, the fingerprints are also used for identification and verification.[10]

Dactyloscopy is based on three laws:

- Around the world are not two people with same
















papillary ridges image;

- Throughout a man's life papillary ridges image remain relatively constant;
- Papillary ridges cannot be removed if is not removed a germ layer of the skin.

Every person has the fingerprint on the surface his or her hands or feet. For fingerprints is also used the term papillary line. They are unique for each person and based on them is possible to recognize an individual person from each other. On the fingertips is possible to find small depressions and elevations.[9] They are created by growing up into the dermis of the skin. The structure of papillary ridges is formed during embryonic development. After, their formation on the surface of the skin remains same for all life. The papillary lines are not located only on hands or feet but also on other parts of the surface of the human body. Papillary lines reaches a height 0,1 – 0,4 mm a width 0,2 – 0,7 mm. [1]

For identification by fingerprints, we focus on the fingerprint minutiae (Table 4). Minutiae are distinguished by their geometric shape, frequency and placement in the papillary ridges image. It is irregular and specific shapes of minutiae that show differences. [11]

Table 1 Fingerprint minutiae [3]

Fingerprint Minutiae	Name	Fingerprint Minutiae	Name
	Dot		Ridge
	Eye		Start and End Ridge
	Island		Hook
	Enclosed Ridge		Fork
	Enclosed loop		Crossing Ridge
	Specialties		Duplication
	Trifurcation		Displacement
			Bifurcation

The advantage of this technology is user friendliness, a large range of sensors and their small dimensions, minimum energy intensity, etc. The disadvantage is the absence of control vividness, so because of that it is easy to bypass the system. At the same time it's easy to get fingerprints without the user's consciousness and for people with dermatological problems is the identification very difficult or sometimes even impossible. [2][3][4]



Fig. 4 Examples of minutiae in fingerprints [3]

### III. MEASUREMENT OF FINGERPRINTS COMPLIANCE

For this measurement was used terminal MorphoSmart Finger VP from Morpho manufacturer. The terminal is connected via USB and individual images were gathered by MorphoEnroll. With this software and terminal were acquired 12 images from each individual subjects. It was about 6 images of left hand and 6 images of right hand (3 images for thumb and 3 for point finger of each hand). The images were converted from RAW14 into BMP format. These images were subsequently adjusted and compared in the eFinger software. That allows comparing two images to determine compliance.

The measurement was attended by 9 family members from 3 families:

- two siblings, their mother and their cousin;
- two siblings and their cousin;
- two siblings.

All 9 people were not intentionally placed in their own name, but all were placed under the names of subject1 to subject9 (in tables as S1 to S9).

For comparison in the eFinger SW were selected only the best and most similar two samples on which were clearly seen the entire finger and the most minutiae papillary ridges and the loop in the middle of finger. The images were taken in two formats (BMP and RAW).

Gradually was selected always one fingerprint at a time. The points have been extracted for each fingerprint and stored in the fingerprint database. After converting of all fingerprints, MIN DISTANCE was chosen as a comparison method. This is the fastest and perhaps the most damning method.

#### A. The measurement of the error rate of scanner

There are two important values for measurement of the error rate of the scanner - False Rejection Rate (FRR) and False Acceptance Rate (FAR), which works with sensitivity values, known as the threshold (Th). For example:

Th = 55 -> FAR = 5,5% and FRR = 1,5% The 5,5% probability of acceptance undesirable person and 1,5%

probability that the device rejects an authorized user (see Fig. 6). Consequently there is a possibility that the unauthorized person can pass through with using of template of authorized user.

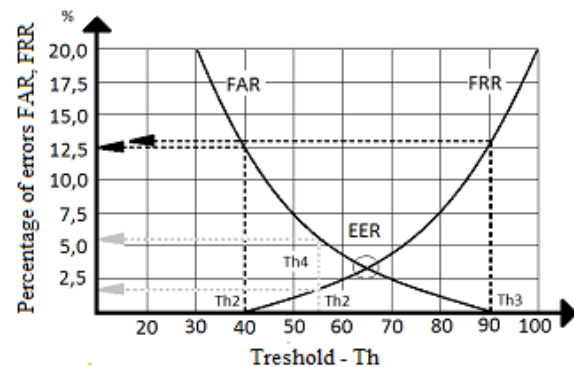


Fig. 5 The dependence FAR and FRR on Th [12]

The measurement was attended by 30 people. Any person was chosen left or right hand, where the left and right hand in the measurement were represented in equal amounts. In next step was captured image of index finger (If) by using a function "Enroll Finger" and subsequently, the images of middle finger (Mf) and ring finger (Rf) - order is not important; by function "Enroll Two Fingers". Two templates from each participant were saved into the database (overall 60 templates). Subsequently, three tests were conducted for identify people. Each person was tested 3 times identification of index finger and 3 times identification according by middle finger or ring finger. Total was held 180 attempts to identify.

Only 7 were incorrect rejections of the total 180 identifications (Table 2.). The level of quality of biometric data ranges from 0 to 40 such very poor quality up to over 120 that is an excellent quality. Excellent quality reached 14 of the 90 samples; very good quality (range 90 to 120) reached 66 samples. Good qualities (range 60-90) were reached by 9 samples. Poor quality (range 40-60) was a single sample, and very bad quality (40) is not appeared.

Table 2. The measured values for the calculation of confidence

Last Name	Hand	Scanned finger		Score			Ident. 1		Ident. 2		Ident. 3	
		If	Mf,Rf	If	Mf	Rf	I f	Mf,R f	I f	Mf,R f	I f	Mf,R f
Subjekt1	R	ok	ok	96	103	120	A	A	N	A	A	A
Subjekt2	L	ok	ok	131	101	108	A	A	A	A	A	A
Subjekt3	R	ok	ok	111	121	126	A	A	A	A	N	A
Subjekt4	L	ok	ok	120	89	100	A	A	A	A	A	A
Subjekt5	R	ok	ok	101	111	100	A	A	A	A	A	A
Subjekt6	L	ok	ok	105	102	107	A	A	A	A	A	A
Subjekt7	R	ok	ok	80	100	59	A	A	A	A	A	A
Subjekt8	L	ok	ok	99	101	117	A	A	A	A	A	A
Subjekt9	R	ok	ok	89	112	92	A	A	A	A	A	A
Subjekt10	L	ok	ok	88	114	89	A	A	A	A	A	A
Subjekt11	R	ok	ok	109	107	121	A	A	A	N	A	A
Subjekt12	L	ok	ok	111	134	116	A	A	A	A	A	A
Subjekt13	R	ok	ok	122	99	113	A	A	A	A	A	A
Subjekt14	L	ok	ok	93	111	100	N	A	A	A	A	A
Subjekt15	R	ok	ok	90	117	103	A	A	A	A	A	A
Subjekt16	L	ok	ok	79	131	96	A	A	A	A	A	A
Subjekt17	R	ok	ok	95	106	92	A	A	A	A	A	A
Subjekt18	L	ok	ok	100	97	114	N	A	A	A	A	A
Subjekt19	R	ok	ok	127	99	110	A	A	A	A	A	A
Subjekt20	L	ok	ok	120	119	123	A	A	A	A	A	A
Subjekt21	R	ok	ok	117	85	97	A	A	A	A	A	A
Subjekt22	L	ok	ok	109	119	110	A	A	A	A	A	A
Subjekt23	R	ok	ok	99	121	115	A	A	A	A	A	A
Subjekt24	L	ok	ok	93	103	114	A	A	A	A	A	N
Subjekt25	R	ok	ok	104	98	100	A	A	A	A	A	A
Subjekt26	L	ok	ok	123	101	90	A	A	A	A	A	A
Subjekt27	R	ok	ok	66	99	116	A	A	A	A	A	A
Subjekt28	L	ok	ok	97	118	94	A	A	A	A	A	A
Subjekt29	R	ok	ok	97	124	95	A	A	A	A	A	A
Subjekt30	L	ok	ok	128	126	111	A	A	N	A	A	A

The calculated FAR came out 0% refer to (1), it indicates that it is hypothetical 0% probability of accepting an unauthorized user by using any finger of any hand. 0% is given by the fact that none of the 60 templates could not log on any unauthorized user. The first 15 participants left 2x15 = 30 templates and 15 others participants tried to log on these templates and then it was the opposite. Nobody could log on to a different template.

$$FAR = \frac{\text{the number of incorrect acceptance}}{\text{the number all attempts of incorrect acceptance}} \cdot 100\% = \frac{0}{60} \cdot 100\% = 0\% \quad (1)$$

Total FRR came out 3.88% refer to (2), which indicates that it is hypothetical 3.88% probability of rejection authorized user using any finger of any hand.

$$FRR \text{ total} = \frac{\text{the number of incorrect rejection any finger and hand}}{\text{the number all attempts to identify any finger and hand}} \cdot 100\% \\ = \frac{7}{180} \cdot 100\% = 3,88\% \quad (2)$$

Total FRR for the left and right hand came out 4.44% refer to (3) and 3.33% refer to (4), thus it is hypothetical 4.44% probability of rejection authorized user using any finger of the left hand and hypothetical 3.33% probability of rejection authorized for use by any finger of the right hand.

$$FRR \text{ total the left hand} = \frac{\text{the number of incorrect rejection any finger of the left hand}}{\text{the number all attempts to identify any finger of the left hand}} \cdot 100\% \\ = \frac{4}{90} \cdot 100\% = 4,44\% \quad (3)$$

$$FRR \text{ total the right hand} = \frac{\text{the number of incorrect rejection any finger of the right hand}}{\text{the number all attempts to identify any finger of the right hand}} \cdot 100\% \\ = \frac{3}{90} \cdot 100\% = 3,33\% \quad (4)$$

Total FRR for index finger and for middle finger / ring finger came out 5.55% refer to (5) and 2.22% refer to (6), therefore it is hypothetical 5.55% probability of rejection authorized user using any index finger and hypothetical 2.22% probability of rejection authorized for use by any middle finger / ring finger.

$$FRR_{I_f} = \frac{\text{the number of incorrect rejection of } I_f \text{ any hand}}{\text{the number all attempts to identify } I_f \text{ any hand}} \cdot 100\% = \frac{5}{90} \cdot 100\% = 5,55\% \quad (5)$$

$$FRR_{M_f, R_f} = \frac{\text{the number of incorrect rejection of } M_f, R_f \text{ any hand}}{\text{the number all attempts to identify } M_f, R_f \text{ any hand}} \cdot 100\% = \frac{2}{90} \cdot 100\% = 2,22\% \quad (6)$$

The FRR for the left index finger and left middle fingers / ring finger came out 6.66% refer to (7) and 2.22% refer to (8), hence it is hypothetical 6.66% probability of rejection authorized user of the left index finger and hypothetical 2.22% probability of rejection authorized for use by left middle finger / ring finger.

$$FRR_{left\ I_f} = \frac{\text{the number of incorrect rejection of } I_f \text{ of the left hand}}{\text{the number all attempts to identify } I_f \text{ of the left hand}} \cdot 100\% = \frac{3}{45} \cdot 100\% = 6,66\% \quad (7)$$

$$FRR_{left\ M_f, R_f} = \frac{\text{the number of incorrect rejection of } M_f, R_f \text{ of the left hand}}{\text{the number all attempts to identify } M_f, R_f \text{ of the left hand}} \cdot 100\% = \frac{1}{45} \cdot 100\% = 2,22\% \quad (8)$$

The FRR for the right index finger and right middle fingers / ring finger came out 4.44% refer to (9) and 2.22% refer to (10), which is indicating the hypothetical 4.44% probability of rejection authorized user using the right index finger and hypothetical 2.22% probability of rejection authorized for use by right middle finger / ring finger.

$$FRR_{right\ I_f} = \frac{\text{the number of incorrect rejection of } I_f \text{ of the right hand}}{\text{the number all attempts to identify } I_f \text{ of the right hand}} \cdot 100\% = \frac{2}{45} \cdot 100\% = 4,44\% \quad (9)$$

$$FRR_{right\ M_f, R_f} = \frac{\text{the number of incorrect rejection of } M_f, R_f \text{ of the right hand}}{\text{the number all attempts to identify } M_f, R_f \text{ of the right hand}} \cdot 100\% = \frac{1}{45} \cdot 100\% = 2,22\% \quad (10)$$

The result from the total number of measurements is fact that the highest probability of rejecting the authorized user is when is used to identification the index finger of the left hand, which is around about 6.66%. The lowest probability of rejection authorized user is when is used to identification any middle finger or ring finger any hand. Here, the probability is about 2.22%.

### B. Results of comparing of fingerprints compliance

For used method MIN DISTANCE is compliance evaluated from 0 to 1000, when 1,000 is the maximum matching (100%). The values above 250 were taken as complying with the minimum number of matching minutiae, which is sufficient for minimum basic agreement that is accepted (Table 3.).

Table 3. Comparison compliance fingerprints between family members

	S1	S2	S3	S4	S5	S6	S7	S8	S9
S1	1000	193							
S2	214	1000							
S3			1000	206	165				
S4			200	1000	146				
S5			231	213	1000				
S6						1000	225	171	182
S7						236	1000	163	195
S8						159	166	1000	274
S9						201	178	183	1000

Similarities with subject1 (193) did not exceed 200, with subject2 (214) was higher when the value exceeds 200. In blue marked group were two siblings (brother – subject4 and sister - subject5) and cousin (subject3). Here the values are slightly higher than the previous group. The highest compliance reaches subject5 that against the other two is above 200 (231 and 213). For subject3 (206 and 165) and subject4 (200 and 146) in one case of both entities value exceeded 200. The average value of the compliance was highest is again in subject5 (148) subject3 (123,66) and subject4 (115,33). Last yellow group had the most representatives. More specifically, it was two siblings (brother – subject9 and sister – subject7), their mother (subject6) and their cousin (subject8). The highest value had subject8 with a value of 274 (compliance between cousin and brother). Average maximum compliance reached subject8 (149,75), followed subject7 (148,5), subject6 (144,5) and subject9 (140,5).

### IV. CONCLUSION

This paper is focusing on the rate of physiological similarities of finger prints between family members. The pattern of papillary lines is formed already during embryonic development, so the fingerprints are partially influenced by the genetic code of the parents. For measurement were used scanner MorphoSmart Finger VP and software MorphoEnroll and eFinger. The measured data show that the similarity of the fingerprints between family members is very small and the possibility of unauthorized access another family member is improbable. If there is any conformity fingerprints between family members, it would be necessary to perform this experiment to a larger sample of people.

## ACKNOWLEDGMENT

With support by grant No. IGA/CebiaTech/2015/044, IGA/FAI/2015/043 and IGA/FAI/2015/039 from IGA (Internal Grant Agency) of Thomas Bata University in Zlin. The work was performed with financial support of research project NPU I No. MSMT-7778/2014 by the Ministry of Education of the Czech Republic, by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089, and by the European Social Fund under the project No. CZ.1.07/2.3.00/30.0035.

## REFERENCES

- [1] Talandová, Hana. Study about application of biometric systems in the industry of commercial security. Zlin, 2010. Bachelor thesis. UTB in Zlin.
- [2] Drahanský, Martin a Filip ORSÁG. Biometrics. 1. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.
- [3] Rak, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. Biometrics and identity of a person in forensic science and commercial applications. 1. Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5.
- [4] LI, Haizhou, Liyuan LI a Kar-Ann TOH. Advanced topics in biometrics. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.
- [5] Baroň, Roman. Use the palmvein finger for biometric identification of individuals.. Zlin, 2014. Diploma thesis. UTB in Zlin.
- [6] Safran Morpho. MorphoAccess VP Series Product Technical Datasheet. Francie, 2012. Available from: [https://www.google.cz/search?q=MorphoAccess\\_VP\\_Series\\_Product\\_Technical\\_Datasheet\\_Rev01\\_3+filetype%3Apdf&aq=MorfoAccess\\_VP\\_Series\\_Product\\_Technical\\_Datasheet\\_Rev01\\_3+filetype%3Apdf&aqs=chrome..69i57.14227j0j7&sourceid=chrome&es\\_sm=93&ie=UTF-8](https://www.google.cz/search?q=MorphoAccess_VP_Series_Product_Technical_Datasheet_Rev01_3+filetype%3Apdf&aq=MorfoAccess_VP_Series_Product_Technical_Datasheet_Rev01_3+filetype%3Apdf&aqs=chrome..69i57.14227j0j7&sourceid=chrome&es_sm=93&ie=UTF-8)
- [7] Biometrics [online]. 2007 [cit. 2010-05-16]. Available from: [www:<http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm>](http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm).
- [8] Kováč, Petr. Esoteric identification, species identification method, device identification technology, development. Zlin, 2007. Bachelor thesis. UTB in Zlin.
- [9] DABBAH, M.A., W.L. WOO and S.S. DLAY. Computationally Efficient Fingerprint Algorithm for Automatic Recognition. Proceedings of the 5th WSEAS Int. Conf. on SIGNAL, SPEECH and IMAGE PROCESSING. Corfu, Greece, 2005, pp90-95.
- [10] VLAD, ALEXANDRA ANISIE a MADALIN STEFAN VLAD. New Developments in Automatic Identification. In: AL], Eds. Nikos Mastorakis ...[et]. Models and methods in applied sciences. Drobeta Turnu Severin: WSEAS Press, 2011, s. 163-166. ISBN 9781618040442.
- [11] MARÁK, PAVOL a ALEXANDER HAMBALÍK. Automated Extraction of Fingerprint Features for Purposes of Analysis of Their Attributes. In: EDITOR, Szabolcs Sergyán. Recent advances in image, audio and signal processing: proceedings of the 9th WSEAS international conference on remote sensing (REMOTE '13), proceedings of the 1st WSEAS international conference on image processing and pattern recognition (IPPR '13), proceedings of the 1st WSEAS international conference on acoustics, speech and audio processing (ASAP '13) : Budapest, Hungary, December 10-12, 2013. 2013, s. 161-170. ISBN 9789604743506.
- [12] BITTO, Ondřej. Encryption and biometrics, or, mysterious bits and touches. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.