

A Preliminary Study of Fake Fingerprints

Qinghai Gao

State University of New York at Farmingdale, New York, USA Email: GaoQJ@farmingdale.edu

Abstract-Fingerprint is a widely used biometrics. Its extensive usage motivates imposter to fabricate fake fingerprints. Vitality detection has been proposed to prevent counterfeit finger attack. Currently the detection can be done either during the process of acquiring fingerprint image or by comparing multiple sequentially acquired images. It is an ongoing research problem to detect whether a given fingerprint image is obtained from a real or a fake fingertip. In this paper we look into the differences between real and fake fingerprints as the first step to approach this problem. Specifically, we study the effects of different imaging sensors on the sizes of templates and on the matching scores between real and fake fingerprints. We also compare the fake fingerprints made from different materials. Experiments are carried out with two publicly available fingerprint databases and the findings are reported.

Index Terms—Fingerprint, minutiae, fake, matching, imaging sensors, fabrication materials.

I. INTRODUCTION

The application of fingerprints for identification has a long history. The earliest fingerprinting of criminals was dated back to 1800BC in Babylon [1]. The usage of finger friction ridges as a proof of identity was recorded around 300BC in ancient China [1] [2]. In the late 19 century friction ridge impression became a popular instrument for crime investigation. The first scientific study of skin friction ridges was published in 1684 [2]. Microscope was first applied to study skin ridges in 1686. The first book on fingerprints was published by Galton [3], who concluded that friction ridge skin was unique and persistent and the odds of two fingerprints being identical were about 1 in 64 billion. In the book Galton [3] described three macroscopic patterns of fingerprints, arch, loop and whorl. Fingerprint evidence helped solve the first homicide murder case in Argentina in 1892 [2]. In 1901 the Henry classification system [4] was developed, which extended the three ridge based patterns depicted by Galton. The first official use of fingerprints in the USA was conducted by the New York City Service Commission in 1901. In 1930 FBI set up national fingerprint files in America. During 1960s automated fingerprint identification systems (AFIS) was being developed, in which the Henry classification was used. State law enforcement agencies started using AFIS in the 1980s. The 1990s saw the emergence of integrated automated fingerprint identification systems (IAFIS). In

2008 FBI initiated the Next Generation Identification (NGI) program to expand the functionality of IAFIS. During the first decade of 21st century, many countries incorporated fingerprints into their machine readable travel documents, such as national ID cards or e-passports [5]. In recent years, some businesses allow their customers to make payments with fingerprints. There are also proposals of using fingerprints for voting [6] [7].

The extensive usages of fingerprints motivate imposters to fabricate fake fingertips and/or counterfeit fingerprints. In fact, the first recorded fingerprint forgery happened in 1920s [8]. It would be desirable for an automated fingerprint system to have the capability of detecting fake fingers. In 1998 Willis and Lee [9] made artificial fingerprints that could fool multiple finger scanners. In 2000 van der Putte and Keuning [10] systematically studied a number of fingerprint scanners and concluded that they could not accurately differentiate real fingers from dummy fingers made from silicone and other materials. In 2002 Matsumoto et al. [11] described procedures of making artificial fingers from gelatin molds. Their experimental results showed that fake fingers can fool all eleven tested fingerprint devices containing optical or capacitive sensors.

The failure of fingerprint devices to detect counterfeit fingers raised serious concerns in biometrics community. In recent years many researchers proposed methods to approach this problem. Jia and Cai [12] proposed a Support Vector Machine based method to differentiate fake fingerprints from real ones. This method analyzes a series of gradually deformed fingerprints and extracts two static features related to perspiration and three dynamic features related to skin elasticity. Derakhshani et al. [13] proposed a perspiration-based method using a series of fingerprints captured within a 5-second time frame. Abhyankar and Schuckers [14] proposed another perspiration-based method using wavelet analysis of two successive fingerprints captured at zeroth second and at fifth second. Tan and Schuckers [15] proposed a detection method by measuring the grey-level intensity distributions and histogram distributions. Antonelli et al. [16] proposed a fake fingerprint detection method based on skin distortion. In this method a user is required to press and rotate the finger on scanner surface. Baldisserra et al. [17] proposed a fake fingerprint detection method by using special sensor to analyze the chemical components of fingerprints. Galbally et al. [18] proposed a detection method based on ten quality features, which relate to ridge strength, ridge continuity, and ridge clarity. Their experimental results showed that this method can successfully classify 90% of the real and fake fingerprints in ATVS-FFb [18] [19] and in LivDet 2009 [20].

Drahansky and Lodrova [21] analyzed human features usable for vitality detection and put them into the following three categories:

Cat-1: Intrinsic characteristics, including light, ultrasonic, and electrical properties. An individual's skin tissue and blood absorb, transmit, and reflect certain amount of lights at certain wave lengths. And human skin tissue reflects ultrasonic waves and has unique electrical properties such as conductance or dielectric constant.

Cat-2: Involuntarily generated signals. It mainly includes pulsation, perspiration/sweat, and body temperature.

Cat-3: Responses to a stimulus. It includes witting responses and involuntary response.

Recently, Drahansky et al. [22] proposed three methods for liveness detection based on pulse measurement (Cat-2), variations of papillary lines induced by pressure change (Cat-3), and skin reaction to illumination with different wavelengths (Cat-1).

Coli [23] divided fingerprint vitality detection methods into the following two categories, hardware-based methods, which require additional hardware to be integrated in to the capturing module in order to measure physiological properties of fingertip, and software-based methods, which extract distinguishing features from fingerprint image(s).

It should be noted that Coli's hardware-based methods focus on detecting vitality during image acquisition stage, while the software based methods attempt to find out if a given fingerprint image is obtained from a live finger or not. To date many commercial fingerprint capturing devices have some built-in mechanisms to detect fake finger during acquisition stage. However, it is a problem far from being solved when it comes to find out the source of a fingerprint, a real or a fake finger. In this paper we look into the differences between real and fake fingerprints as the first step to approach this problem. In addition, we compare fake fingerprints made from different materials.

The rest of the paper is organized as the following. Section II briefly describes the minutia-based fingerprint matching mechanisms. The *Bozorth* program [24] from NIST and the *VeriFinger* [25] from *Neurotechnology* are used to match fingerprint minutiae templates. Section III presents the experimental results obtained with two datasets: ATVS-FFp DB [18] [19], and the Clarkson-Cagliari Joint Multi-modal Biometric Dataset [20] [26]. Section IV summarizes the paper and proposes possible future research topic.

II. METHODS

A typical fingerprint system contains four subsystems, including acquisition, feature extraction, matching, and decision making. An image produced by the acquisition subsystem is processed and then a template is extracted from the processed image. The template consists of a number of points called minutiae. Most minutiae are points of ridge ending or ridge bifurcation (Refer to Fig. 1). Every minutia is represented with one triple (x, y, θ) , where (x, y) is a minutia's Cartesian coordinates, and θ is the ridge orientation at the point. During matching one template will be matched against another template to produce a numerical score. A user-selected threshold is needed to decide whether the two templates match successfully or not.



Fig.1. Designation of fingerprint minutiae

In this paper the fingerprints in the ATVS-FFp database are matched with the Bozorth algorithm, which consists of three major steps [24] [27]:

- 1) Transform a minutiae template into an intrafingerprint minutia comparison table (CT) In a template, for each pair of minutiae, a five-variable entry including the length (*d*) of the line segment between the two minutiae ($\alpha 1$, $\alpha 2$) and the angles ($\beta 1$, $\beta 2$) between each minutia and the line connecting the two minutiae, is made into a CT. Two CTs are constructed from a pair of to-bematched fingerprints. One is called the registered CT and the other is called the query CT.
- 2) Construct inter-fingerprint minutia compatibility tables Compare each entry in the registered fingerprint's CT to the entries in the query fingerprint's CT. If the differences (Δd) between the lengths of the two segments and those of the corresponding angles ($\Delta\beta 1$, $\Delta\beta 2$) are smaller than or equal to the predefined thresholds, an entry representing the two pairs of minutiae will be made into the inter-fingerprint minutia compatibility table.
- 3) Traverse the inter-fingerprint compatibility tables to obtain a matching score between the two fingerprints. More details about the algorithm can be found in [28].

The fingerprints from the Clarkson-Cagliari Joint Multi-modal Biometric Datasets [26] are matched with another proprietary algorithm, VeriFinger [25]. Similar to the Bozorth algorithm [24], it matches two fingerprints based on their minutiae templates.

III. RESULTS

The ATVS-FFp datasets [18] [19] contain paired fingerprints acquired from real fingers and their

corresponding fake ones. The fake fingers were made as follows. The users were divided into two groups. For the first group fake fingers were made directly from their real fingers – user cooperation. For the second group fake fingers were made from their fingerprint images – no user cooperation. Four fingerprint images are captured from every finger, fake or real, with each of the three types of sensors: capacitive, optical, and thermal. With the minutia detection algorithm given in the NIST fingerprint software [24], a minutia template is generated for every fingerprint in the datasets. Matching is carried out between two templates as described in Section II. The results are given below.

A. Effects of sensor types on minutia counts

Fig. 2 gives the minutiae count distributions of the individual templates.



Fig.2. Comparison of fake and real fingerprint minutiae count distributions



Fig.3. Sensor-based fingerprint minutiae count distributions

From Fig. 2, it can be seen that among the three types of sensors the fake fingerprints generated by the capacitive sensor tend to have significantly larger number of minutiae than their corresponding real fingerprints. The results in Fig. 2 also verify that with user cooperation the minutiae counts of the fake fingerprints are closer to the counts of the real fingerprints than to those without user cooperation.

From Fig. 3 it can be seen that the capacitive sensor (marked with blue diamonds) produces fingerprints with narrower minutiae count distributions than both the optical sensor (marked with red squares) and the thermal sensor (marked with green circles) do. It also shows that the optical sensor tends to produce fingerprints containing the largest numbers of minutiae.

Table 1 lists the ranges and averages of minutiae counts for all the fingerprints in ATVS-FFb. These results are consistent with the observations made from Fig. 2 and Fig. 3.

Sensor Type		Capacitive	Optical	Thermal	
	Range	21~102	63~171	34~179	
Real					
	Average	48	112	74	
	Range	46~108	38~158	15~130	
Fake-Coop					
· F	Average	79	105	70	
	Range	18~89	28~359	32~179	
Real					
	Average	45	96	65	
	Range	48~135	23~161	32~167	
Fake-NoCoop					
	Average	88	80	87	

Table 1. ATVS-FFb Fingerprint Templates Minutiae Count Summary

Τ

Т

B. Effects of sensor types on matching scores

The matching results between real and fake fingerprints are given in Fig. 4. The curves marked with blue diamonds are the results of matching real fingerprints with fake ones with user cooperation, while these marked with red stars are obtained without user cooperation. It can be seen that the highest peaks for all three blue curves are shifted to the right-hand side and are lower than these for the red curves. These results prove the fact that user cooperation helps making fake fingers more similar to the real ones.

Fig. 5 compares the matching results under user cooperation for the three types of sensors. It can be seen that the optical sensor produces the highest matching scores while the capacitive sensor produces the lowest matching scores. The matching scores generated by the thermal sensors lie in between.



Fig.4. Sensor-based score distributions



Fig.5. Score distributions with user cooperation

Г

C. Effects of different materials on making fake fingers

Different types of materials have been used to make artificial/fake fingertips with user cooperation. The Joint Multi-modal Biometric Dataset [26] contains fingerprint images generated from fake fingertips made from five different materials: EcoFlex, Gelatine, Latex, Silgum, and WoodGlue. To find out which material is the best for making fake fingers, we randomly choose six fingers (A, B, C, D, E, & F) from the datasets, each of which has five images captured from its real finger and ten fake images captured from a fake finger made from each material mentioned above. For example, Finger #A has five real images, 10 fake images from EcoFlex, 10 fake ones from Gelatine, 10 fake ones from Latex, 10 fake ones from Silgum, and 10 fake one from WoodGlue. The average matching scores obtained with VeriFinger [25] are sorted numerically and then plotted in Fig. 6.



Fig. 6. Matching results for Finger #A-F (Vertical axis - matching score, Horizontal axis - sequence number)

Table 2 summarizes the results plotted in Fig. 6.

Table 2. Material Bas	ed Average M	atching Scores
-----------------------	--------------	----------------

Finger	EcoFlex	Gelatine	Latex	Silgum	WoodGlue	Real
А	435.4	292.4	485.7	524.0	458.9	617.9
В	373.4	174.1	480.2	362.2	299.4	567.0
С	296.9	476.5	353.9	379.3	480.1	763.1
D	328.3	233.3	375.5	259.9	304.3	525.0
Е	578.1	359.1	503.6	483.9	255.4	681.4
F	406.0	136.0	394.2	443.1	503.7	787.6
Overall Average	403.0	278.6	432.2	408.7	383.6	657.0

The highlighted numbers in Table 2 signify the best material for that particular finger in that row. For example, the best material to make fake finger for Finger #A is Silgum, which gives the highest matching score 524.0 among all the materials. If one and only one material has to be selected to make fake fingers for all six fingers listed in Table 2, Latex will be chosen because it gives the highest overall average score 432.2 (as shown in the last row of Table 2). The results indicate that different materials have different capacity at capturing the fine details of human fingerprints.

Non-material related factors may also need to be taken into account. Without knowing the details of making the artificial fingertips for the fake fingerprints in the dataset, we assume that similar procedures to those reported by Matsumoto et al. [11] were utilized. Therefore, we believe, in accordance with the observations made in [16] [29] [30] [31] [32], some extents of elastic deformations would have happened unavoidably during the fabrication processes. The projection from fake 3D fingertips to 2D fingerprint images, as indicated in [33] [34] [35] [36] [37] [38] [39], can also lower matching score or cause nonmatch. Therefore, possible future research topics include looking into the elasticity of different materials and matching fake 3D fingerprints with real 3D fingerprints.

IV. CONCLUSIONS

It is still an ongoing research problem to detect whether a given fingerprint image is obtained from a real or a fake fingertip. Currently, fingerprint vitality detection can be done with limited accuracy either in the process of capturing image or by comparing a series of sequentially acquired images. We believe that looking into the differences between fake and real fingerprints is the very first step to find a solution to the challenging problem.

In this paper we carried out experiments with two fingerprint databases. The following three conclusions can be drawn from the results:

- The type of sensor used for image capturing significantly affects fingerprint minutiae templates. Capacitive sensor tends to introduce false minutiae fake fingerprints captured with capacitive sensor tend to have significantly larger number of minutiae than their corresponding real fingerprints do. Optical sensor tends to produce fingerprints containing the largest number of minutiae, compared to capacitive and thermal sensors.
- The type of sensor significantly affects the matching between a real fingerprint and its corresponding fake fingerprint. Optical sensor produces the highest matching scores while the capacitive sensor gives the lowest matching scores.
- Fake fingers made from different materials produce significantly different results. However, among the five materials studied, it seems that no material can be used to make the best fake fingers for all the real

fingers. Other factors including elastic distortion and the 3D-to-2D projection may also affect the results.

Future research may be conducted in the following directions: using larger databases containing images captured with more varieties of sensors; using composite materials with specified elasticity to refine the processes of fake fingerprint fabrication; and using 3D fingerprints for matching.

ACKNOWLEDGMENT

The author wishes to thank Dr. Javier Galbally from Autonomous University of Madrid for providing access to the ATVS-FFb fingerprint database, and to thank Dr. Stephanie Schuckers at Clarkson University for providing access to the LivDet 2011 fingerprint database.

REFERENCES

- J. Barnes, Chapter 1 History. *The Fingerprint Sourcebook*, Alan McRoberts, Eds, National Institute of Justice, 2012, pp. 7-21.
- [2] David R. Ashbaugh, "Ridgeology," *Journal of Forensic Identification*, vol. 41, no. 1, pp. 16-64, 1991.
- [3] F. Galton, *Finger Prints*, MacMillan and Co, London, 1892.
- [4] L. Hutchins, Chapter 5 Systems of friction ridge classification. *The Fingerprint Sourcebook*, Alan McRoberts, Eds, National Institute of Justice, 2012, pp. 8-9.
- [5] V. Narendira Kumar and B. Srinivasan, "Evolution of electronic passport scheme using cryptographic protocol along with biometrics authentication system," *International Journal of Computer Network and Information Security*, vol. 2, pp. 50-58, 2012.
- [6] D. Gentles and S. Sankaranarayanan, "Application of biometrics in mobile voting," *International Journal of Computer Network and Information Security*, vol. 7, pp. 57-68, 2012.
- [7] D. Ashok Kumar and T. Ummal Sariba Begum, "A novel design of electronic voting system using fingerprint," *International Journal of Innovative Technology & Creative Engineering*, vol. 1, no. 1, pp. 12-19, 2011.
- [8] S. Cole, Suspect Identitites: A History of Fingerprinting and Criminal Identification, Harvard University Press, 2001.
- [9] D. Willis and M. Lee, "Six biometric devices point the finger at security," *Computers and Security*, vol. 17, no. 5, pp. 410-411, 1998.
- [10] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," *Smart Card Research and Advanced Applications*, Springer, 2000, pp. 289-303.
- [11] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," *Electronic Imaging*, pp. 275-289, 2002 International Society for Optics and Photonics.
- [12] J. Jia and L. Cai, "Fake finger detection based on timeseries fingerprint image analysis," Advanced Intelligent Computing Theories and Applications, With Aspects of Theoretical and Methodological Issues, 2007, pp. 1140-1150. Springer Berlin Heidelberg.
- [13] R. Derakhshani, S. Schuckers, L. A., Hornak, and L. O'Gorman, "Determination of vitality from a non-invasive

biomedical measurement for use in fingerprint scanners," *Pattern Recognition*, vol. 36, no. 2, pp. 383-396, 2003.

- [14] A. Abhyankar and S. Schuckers, "A wavelet-based approach to detecting liveness in fingerprint scanners," *Defense and Security*, pp. 278-286, 2004 International Society for Optics and Photonics.
- [15] B. Tan and S. Schuckers, "Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners," *Proc. SPIE*, 2006, pp. 62020A-62020A. Biometric Technology for Human Identification III.
- [16] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 360-373, 2006.
- [17] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," *Advances in Biometrics*, 2005, pp. 265-272. Springer Berlin Heidelberg.
- [18] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 311-321, 2012.
- [19] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *Telecommunication Systems*, vol. 47, no. 3-4, pp. 243-254, 2011.
- [20] G. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers, "First international fingerprint liveness detection competition livdet 2009," *Image Analysis and Processing*, pp. 12-23. Springer Berlin Heidelberg.
- [21] M. Drahansky and D. Lodrová, "Liveness detection for biometric systems based on papillary lines," *International Conference on Information Security and Assurance*, 2008, pp. 439-444.
- [22] M. Drahansky, M. Dolezel, J. Vana, E. Brezinova, J. Yim, and K. Shim, "New optical methods for liveness detection on fingers," *BioMed research international*, 2013, pp. 1-11.
- [23] P. Coli, "Vitality detection in personal authentication systems using fingerprints," Doctoral Thesis, 2008, University of Cagliari.
- [24] NIST fingerprint software. Available at: http://fingerprint.nist.gov/nfis/
- [25] VeriFinger from Neurotechnology. Available at: http://www.neurotechnology.com/
- [26] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011—fingerprint liveness detection competition," *The 5th IAPR International Conference on Biometrics*, 2012, pp. 208-215.
- [27] S. N. Srihari, H. Srinivasan, and G. Fang, "Discriminability of fingerprints of twins," *Journal of Forensic Identification*, vol. 58, no. 1, pp. 109-127, 2008.
- [28] C. I. Watson, M. D. Garris, and A. Hicklin, "Studies of fingerprint matching using the NIST verification test bed (VTB)," US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2003.
- [29] A. Ross, S. Dass, A. Jain, "A deformable model for finger-print matching", *Pattern Recognition*, vol. 38, pp. 95-103, 2005.
- [30] R. Cappelli, D. Maio, and D. Maltoni, "Modelling plastic distortion in fingerprint images," Proc. Second International Conference on Advances in Pattern Recognition, pp. 369-376, 2001.

- [31] Q. Gao and X. Zhang, "A study of distortion effects on fingerprint matching," *Computer Science and Engineering*, vol. 2, no. 3, pp. 37-42, 2012.
- [32] H. da Costa, J. Maxey, L. Silva, and A. Ellerbee, "Evaluation of fingerprint deformation using optical coherence tomography," *Proc. SPIE*, *Optical Elastography and Tissue Biomechanics*, 2014, pp. 894601.
- [33] Q. Zhao, A. Jain, and G. Abramovich, "3D to 2D fingerprints: unrolling and distortion correction," *IEEE International Joint Conference on Biometrics* (IJCB), 2011 pp. 1-8.
- [34] Y. Wang, D. Lau, and L. Hassebrook, "Fit-sphere unwrapping and performance analysis of 3D fingerprints," Applied Optics, vol. 49, no. 4, pp. 592-600, 2010.
- [35] R. Labati, A. Genovese, V. Piuri, and F. Scotti, "Contactless fingerprint recognition: a neural approach for perspective and rotation effects reduction," *IEEE Workshop on Computational Intelligence in Biometrics and Identity Management* (CIBIM), 2013, pp. 22-30.
- [36] R. Labati, A. Genovese, V. Piuri, and F. Scotti, "Virtual environment for 3-D synthetic fingerprints," *IEEE International Conference on Virtual Environments Human-Computer Interfaces and Measurement Systems* (VECIMS), 2012, pp. 48-53.
- [37] F. Liu, D. Zhang, C. Song, and G. Lu, "Touchless Multiview Fingerprint Acquisition and Mosaicking," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 9, pp. 2492-2502, 2013.
- [38] R. Labati, A. Genovese, V. Piuri, and F. Scotti, "Touchless fingerprint biometrics: a survey on 2D and 3D technologies," *Journal of Internet Technology*, vol. 15, pp. 325-332, 2014.
- [39] R. Labati, A. Genovese, V. Piuri, and F. Scotti, "Accurate 3D fingerprint virtual environment for biometric technology evaluations and experiment design," *Proc. IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications* (CIVEMSA), pp. 43-48. 2013.

Author Profile



Qinghai Gao, born in Shandong China in 1969, received a Ph.D. in computer science from the City University of New York in 2007.

He is an Associate Professor in the Department of Security Systems & Law Enforcement Technology at Farmingdale State College. Before joining Farmingdale, he taught full-

time in the China University of Petroleum for a few years. From 1998 to 2007 he taught as Adjuncts in Brooklyn College, Lehman College, NYC College of Technology, College of Staten Island, and York College. Since 2001 he held various positions in IT industry as Software Developer, Database Administrator, Network Engineer, Researcher, Consultant, and Information Security Specialist. He has extensive experience with forensic fingerprint recognition, biological information system, and cryptography. He has published one book and numerous articles. His present research interests include Digital Forensics, Computer Security, Biometrics, Cryptography, and Bioinformatics.

Dr. Gao is a current member of following professional organizations: International Association of Identification (IAI), Association of Computing Machinery (ACM), International Association of Computer Investigative Specialists (IACIS), and High Technology Crime Investigation Association (HTCIA). Manuscript received May 29, 2014; revised Sept. 18, 2014; accepted xx, 2014.

How to cite this paper: Qinghai Gao,"A Preliminary Study of Fake Fingerprints", IJCNIS, vol.6, no.12, pp.1-8, 2014. DOI: 10.5815/ijcnis.2014.12.01