Detection From Fingerprint Images A Critical Section To Analyze the State Of the Art and the Related Open Issues.

Asst. Prof. M. Sreenivas, Mr. Shimpi Jaiprakash Bhika

Abstract.-**Although fingerprint verification systems reached a high degree ofaccuracy, it has been recently shown that they can be circumvented by "fakefingers", namely, fingerprint images coming from stamps reproducing an userfingerprint, which is processed as an "alive" one. Several methods have beenproposed for facing with this problem, but the issue is far from a final solution.Since the problem is relevant both for the academic and the industrialcommunities, in this paper, i present a critical review of current approaches tofingerprint vitality detection in order to analyze the state–of–the art and therelated open issues**.

Keywords- **fake fingers,shape,static,dynamic,fingerprint detection**

1 INTRODUCTION

In the last years, fingerprint verification systems for personal identity recognitionreached a high degree of accuracy [1]. Fingerprints can be reasonably considered thebiometric for which academic and industrial research achieved the highest level ofmaturity. In fact, many capture devices have been implemented with powerfulsoftware development kits for acquiring, processing and matching fingerprint images.The reason of this success is mainly due to the most claimed characteristic offingerprints: their uniqueness [2]. In other words, it is claimed that fingerprints areunique from person to person, and the probability to find two similar fingerprintscharacterized, for example., by minutiae is very low [2].However, recent works pointed out that the current fingerprint capture devices canbe deceived by submitting a "fake fingerprint" made up of gelatin or liquid silicon[3]. This fake finger can be obtained by person coercion (the so-called "consensual"method) or by latent fingerprints [3]. The first method is the most simple, as itrequires that the person put his finger on a plasticine-like material. The next step is todrip over this mould some liquid silicon. After its solidification, a fake stampreproducing the fingerprint of the client can be used for deceiving the acquisitionsensor, which processes that as an "alive" fingerprint. An example of "live" and"fake" fingerprint images fabricated by the consensual method and acquired with anoptical sensor is given in Figure 2. Obviously, reproducing a fingerprint is not so easyas it may appear, because high quality stamps are necessary for a successful logon on a system protected with a fingerprint authentication module. On the other hand, theissue exists, as it was pointed out in [3].

II Fingerprint vitality detection: a taxonomy of existing methods

A possible taxonomy of fingerprint vitality detection methods is proposed in Figure 1.Roughly, existing approaches can be subdivided in "hardware-based" and "softwarebased".The first ones try to detect the vitality of the fingertip put on the sensor byadditional hardware able to measure, for example, blood pressure [4], heartbeat [5],fingertip odor [6], or skin impedance [7]. These approaches are obviously expensiveas they require additional hardware and can be strongly invasive: for example,
measuring person's blood pressure is invasive as it can be used for other reasons thatfor simply detecting the vitality of his fingertip [8]. Moreover, in certain cases aclever imitator can circumvent these vitality detection methods.Therefore, making the image processing module more "intelligent", that is, makingit able to detect if a fake finger has been submitted is an interesting alternative to thehardware-based approaches. Several approaches aimed to extract vitality featuresfrom the fingerprint images directly have been recently proposed [9-15]. The generalrationale behind these approaches is that some peculiarities of "live fingerprints"cannot be hold in artificial reproductions, and they can be detected by a more or lesscomplex analysis of fingerprint images. The related vitality detection approaches canbe named "software-based".
According to the taxonomy of Figure 1, the initial subdivision of the softwarebasedapproaches is based on the kind of features used. If the features extracted derivefrom the analysis of multiple frames of the same image, captured while the subjectputs his fingertip on the acquisition surface at certain time periods (e.g., at 0 sec andat 5 sec), the related methods are named "dynamic" (as they use dynamic features) .On the other hand, if features are extracted from a single fingerprint impression or theComparison of different impressions, the methods are named "static"(as they use staticfeatures).Referring to the leaves of the taxonomy in Figure 1, they describe software-

ISSN: 2278 – 1323

basedapproaches as functions of the physical principle they exploit: the perspiration, theelastic distortion phenomena, and the intrinsic structure of fingerprints(morphological approaches).

According to the proposed taxonomy, in the following sections, review thevitality detection methods proposed in the scientific literature.

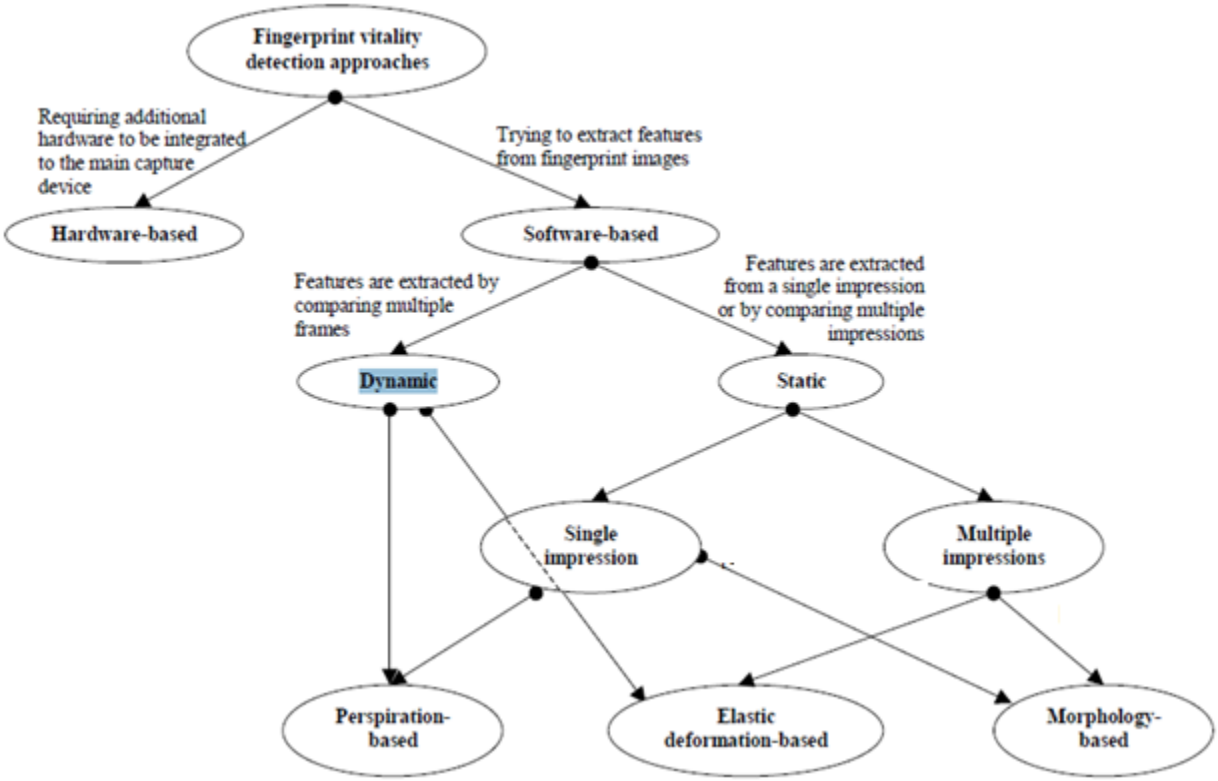

Figure. 1. The proposed taxonomy of fingerprint vitality detection methods. Labels of the edges in the form [*] are the number of the related Reference.

III STATIC METHODS

A. Static methods using a single impression

The rationale of this method is the analysis of the Particularshape of the finger surface. In live fingers, in order to guarantee thephysiological thermo-regulation, there are many little chinks named "pores" scatteredalong the center of the ridges. Because of this characteristic the acquired image of a Figure shows a non-regular shape of the ridges. Generally the path of the ridges isirregular and, if the resolution of the device is high enough, it is possible to observethese pseudo-periodic conformations at the center of the ridges. With the fabricationstep of an artificial finger it is possible to lose these micro-details and consequentlythe correspondent acquired image is more regular in the ridge shape. The authors Propose to analyze this feature with wavelet decomposition. In particular, the imageis enhanced and converted into a mono-dimensional signal as the gray level profileextracted in correspondence of the center of the ridges. A wavelet decomposition ofthis signal is applied with a five-levels multiresolution scheme:

The standarddeviation, the mean value for each wavelet coefficient and from the original and the last approximation signals are computed. The obtained 14 parameters are consideredas a feature-vector for the next classification stage.The concept of detecting liveness from the skin perspiration analysis of the poreshas been already proposed in [9]. In particular, the authors uses one static feature, named*SM*, based on the Fast Fourier Transform of the fingerprint skeleton convertedinto a mono-dimensional signal. The rationale is that for a live finger it is possible tonotice clearly the regular periodicity due to the pores on the ridges. On the contrarythis regularity is not evident for spoof fingerprint signals.Carrying on with single impression-static methods, another work is noticeable tomention. Unlike the previous works, this applies a liveness detection studying themorphology of the fingerprint images. So, referring to Figure 1, the branch ending tomorphologic based method is related to the work by Moon et al. [11].

The study is based on a different method with a contrasting argument. Looking atthe finger

ISSN: 2278 – 1323

surface with an high resolution Digital Single Lens Reflex camera, theyobserve that the surface of a fake finger is much coarser then that of a live finger. Themain characteristic of this work is that an high resolution sensor is necessary forsuccessfully capturing this difference (1000 dpi, whilst current sensors exhibit 500 dpion average). Moreover, this approach does not work with the entire image, too largebecause of its resolution, but with subsamples of a fixed size. For extracting thisfeature, the residual noise returned from a denoising-process applied to the originalsub-images is considered. The standard deviation of this noise is then computed to highlight the difference between live and fake coarseness.

III. STATIC METHODS USING MULTIPLE IMPRESSIONS

Whilst the previous studies search a liveness indication from intrinsic properties ofa single impression, there are other static features based on multiple impressions: inthis case the liveness is derived from a comparison between a reference templateimage and the input image. This methods are represented in Figure 1 with twobranches starting from the "Multi-impressions" node: one indicates method based onelastic-deformation features, the other indicates ones based on morphologic features.
Ref [10] falls within the first category. Given a genuine query-template pair offingerprints, the entity of elastic distortion between the two sets of extracted minutiaeis measured by a thin-plate spline model. The idea is that live and spoof fingerprintsshow different elasticity response repeating the acquisitions.

IV DYNAMIC METHODS

Dynamic methods for vitality detection relies on the analysis of different imageframes acquired during an interval while the user put his finger on the scanner.As it is schematized in Figure 1 there are two types of dynamic methods: one based on the perspiration phenomenon, the other on the elastic response of the skin.The same properties of the skin used for a static measure in [9, 11] is exploitedwith dynamic analysis based on the first approach [9]: the pores scattered on thefingertip surface are the source of the perspiration process. When the finger is incontact with the surface of the scanner, the skin gets bitter because of an increasing ofsiat amount. This physiological phenomenon can be recorded by acquiringsequential frames during a fixed interval of few seconds. The variation of the itnessof the fingertip skin reflects on a variation of the gray-level profile of the acquiredimages. In order to evaluate this feature, the fingerprint skeleton of the image at 0 and5 seconds is converted into a couple of mono-dimensional signals (C1, C2). Severalstatistical measures are proposed on the basis of the obtained signals. In particular [9],DM1 (Total swing ratio), DM2 (Min/Max growth ratio), DM3 (Last-First fingerprintsignal difference mean), DM4 (Percentage change of standard deviation).
However, it should be noted that several variables are involved in the fraudulentaccess process, in particular: (1) the initial pressure of the subject on the cast; (2) themould material dripped over the cast; (3) the contact of the stamp on the acquisitionsurface. These variables concur to alter the shape of the reproduced fingerprint and, insome cases, these alterations strongly impact on the final quality of the obtainedimage. Figure 2 shows some examples of fake fingerprint images where it can beeasily observed the different visual quality. It is worth noting that no previous workhas devoted much attention to this issue. However, in our opinion, it is importantbecause adding a fake fingerprint detector obviously impacts on the false rejectionrate of the system, that is, the rate of genuine rejected due to misclassified livefingerprints. Fake fingerprint images of poor quality, as those showed in Figure 2(a,c), could be easily rejected without employing a fake detector. It is worth noting thatthis problem arises independently on the position of the fake detection module intothe processing chain (e.g. if the fake detection is done before or after the verification stage).

V .FABRICATION PROCESS OF FAKE STAMPS AND DATA SETS USED

I believe that a critical review of previous works on fingerprint vitality detectionshould analyze: (i) the different materials employed for fake stamps and the methodsused for creating them; (ii) the characteristics of the data sets used for the vitality detection experiments. Item (i) is important because the response of a certain fingerprint scanner varies with thematerial adopted (e.g., gelatine or silicon). Secondly, the intrinsic quality of the stampdepends on the material for the cast and the method followed for its creation. With regard to the mould materials, all those employed are able to deceive an opticalsensor, as pointed out in [3]. On the other hand, using the silicone material is noteffective for capacitive sensors, probably due to the different electrical properties ofthis material with respect to the skin.However, it should be noted that several variables are involved in the fraudulentaccess process, in particular: (1) the initial pressure of the subject on the cast; (2) themould material dripped

ISSN: 2278 – 1323

over the cast; (3) the contact of the stamp on the acquisitionsurface. These variables concur to alter the shape of the reproduced fingerprint and, insome cases, these alterations strongly impact on the final quality of the obtainedimage. Figure 2 shows some examples of fake fingerprint images where it can be easily observed the different visual quality. It is worth noting that no previous workhas devoted much attention to this issue. However, in our opinion, it is importantbecause adding a fake fingerprint detector obviously impacts on the false rejectionrate of the system, that is, the rate of genuine rejected due to misclassified livefingerprints. Fake fingerprint images of poor quality, as those showed in Figure 2(a,c), could be easily rejected without employing a fake detector. It is worth noting thatthis problem arises independently on the position of the fake detection module intothe processing chain (e.g. if the fake detection is done before or after the verification stage).

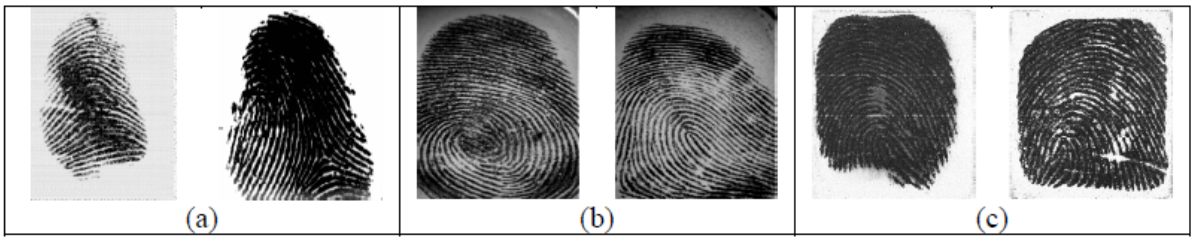

Figure. 2.*Examples of fake fingerprint images*

analyze: (1) the sample size of data setsfor fake detection rate evaluation; (2) the protocol adopted in experiments.With regard to item (1), it is worth noting that it requires several resources in termsof volunteers, time, and personnel devoted to stamp fabrication. In particular,volunteers must be trained to appropriately press their finger on the mould material,and a visual analysis of the stamp is necessary in order to obtain good quality images.
In order to produce an acceptable stamp, many trials are required. Since thesolidification of the mould material can require several hours, this impacts on the number of fake stamps produced per time unit. As a consequence, reportedexperimental results can be affected by the small sample size of the used data set. This could cause a not reliable estimation of the detection performance.

VI CONCLUSION

Fingerprint vitality detection has become a crucial issue in personal verificationsystems using this biometric.In this paper, i critically revived the main approaches to fingerprint vitalitydetection proposed in these years. To the best of our knowledge, this is the firstsurvey about fake fingerprint detection methods. In particular, i proposed a possibletaxonomy for summarizing the current state-of-the-art and also examined thescientific literature from other point of views, as the materials employed forproducing fake stamps and the data sets used for experiments. Finally, i reported thedetection rates of previous works in order to trace a preliminary comparison amongthe current approaches.Our future work will analyze further the state of the art and will also perform a fair
Experimental comparison by adopting an appropriate data set aimed to highlight prosand cons of the state-of-the-art methods for fingerprint vitality detection.

REFERENCES

[1] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of fingerprint recognition,Springer, (2003).
[2] R.M. Bolle, J.H. Connell, N.K. Ratha, Biometric perils and patches, Pattern Recognition35(12): 2727-2738 (2002).
[3] T. Matsumoto, H. Matsumoto, K. Yamada, H. Hoshino, Impact of artificial 'gummy' fingers on fingerprint systems, Proceedings of SPIE, vol. 4677, (2002).
[4] P. Lapsley, J. Less, D. Pare, N. Hoffman, Anti-Fraud Biometric Sensor that AccuratelyDetects Blood Flow, SmartTouch, LLC, US Patent #5,737,439, (1998).
[5] L. Biel, O. Pettersson, L. Philipson, P. Wide, ECG analysis: A new approach in humanidentification, IEEE Transactions on Instrumentation and Measurement 50 (3) 808-812
(2001).
[6] D. Baldissera, A. Franco, D. Maio, D. Maltoni, Fake Fingerprint Detection by OdorAnalysis, in proceedings International Conference on Biometric Authentication (ICBA06),Hong Kong, January (2006).
[7] D. Osten, H.M. Carim, M.R. Arneson, and B. L. Blan, Biometric, Personal AuthenticationSystem, U.S. Patent #5 719 950, Feb. 17, (1998).
[8] A.K. Jain, R. Bolle and S. Pankanti (Eds.), BIOMETRICS: Personal Identification inNetworked society, Kluir Academic Publishers, (1999).
[9] R. Derakhshani, S. Schuckers, L. Hornak , L. O'Gorman, Determination of vitality from anon-invasive biomedical measurement for use in fingerprint scanners, Pattern Recognition36 (2) (2003) 383-396.
[10] Y. Chen, A.K. Jain, S. Dass, Fingerprint deformation for spoof detection, BiometricSymposium, Cristal City, VA, (2005).
[11] Y.S. Moon, J.S., Chen, K.C. Chan, K. So, K.C. Woo1, Wavelet based fingerprint livenessdetection. Electronics Letters, 41 (20) (2005) 1112-1113.

ISSN: 2278 – 1323