Fake Fingertip Generation from a Minutiae Template

Javier Galbally[2], Raffaele Cappelli[1], Alessandra Lumini[1], Davide Maltoni[1], Julian Fierrez[2]

[1]*Biometric Systems Laboratory - DEIS,Università di Bologna*
{cappelli, lumini, maltoni}@csr.unibo.it
[2]*Biometric Recognition Group - ATVS, Universidad Autonoma de Madrid*
{ javier.galbally, julian.fierrez}@uam.es

Abstract

This work reports a preliminary study on the vulnerability evaluation of fingerprint verification systems to direct attacks carried out with fake fingertips created from minutiae templates. The attack is performed by presenting to the acquisition sensor a fake fingertip generated from an image reconstructed from a compromised minutiae-based template. Experiments carried out against a state-of-the-art fingerprint recognition algorithm show that the proposed attack scheme is definitely feasible and highlight a potential security threat in the use of non-encrypted minutiae-based templates.

1. Introduction

Fingerprints are one of the most used biometrics in automatic identity verification systems, since they have many desirable properties: universality, high distinctiveness, high accuracy in recognition and durability throughout lifetime [10]. However, in spite of their numerous advantages, fingerprint biometric systems are vulnerable to direct and indirect attacks, which can decrease their security. Direct attacks are carried out using a fake biometric trait with the only requirement of having access to the sensor [5][13], while indirect attacks exploit some knowledge about the internal functioning of the system to deceive one or more of its inner modules [15].

Fingerprint recognition in automated verification systems is typically based on minutiae and local ridge-line orientations, which are both stable and robust to fingerprint impression conditions [10]. Since a minutiae-template is an extremely compact representation of the fingerprint, the thought that this type of templates does not comprise enough information to reconstruct the original fingerprint image was generalized (i.e., the template extraction procedure has been traditionally considered a one-way function). However, this belief has been recently questioned in [2] where the reversibility of minutiae templates was explored. In that work, reconstructed images from standard ISO templates were successfully used to spoof different fingerprint based recognition systems through an indirect attack (e.g. sending the reconstructed image to the feature extraction module of the system).

The aim of this work is to evaluate the possibility of performing a direct attack (i.e. to the acquisition sensor) using fake fingertips made from an image reconstructed from a "stolen" template. This way an indirect attack to the input of the feature extractor could be transformed into a far less demanding direct attack to the sensor.

The rest of the paper is organized as follows: Sect. 2 summarizes the main steps of the reconstruction approach from the minutiae template to the fake fingertip; Sect. 3 reports and discusses the experimental results, and conclusions are finally drawn in Sect. 4.

2. The Reconstruction Approach

The fake finger reconstruction approach evaluated in this work comprises two phases: (*i*) the fingerprint image is generated according to the technique proposed in [2], and (*ii*) the reconstructed fingerprint image is used to make the fake fingertip.

The image reconstruction approach exploits the information stored in the template to reconstruct a

978-1-4244-2175-6/08/$25.00 ©2008 IEEE

realistic image by estimating several aspects of the original unknown fingerprint (Fig. 1).

Templates with two different levels of information are considered in this work:

- MINTYPE: containing only minutiae data stored as a Fingerprint Minutiae Record [7].
- ORIMG: containing information on the local ridge-line orientation in addition to the ISO minutiae data.

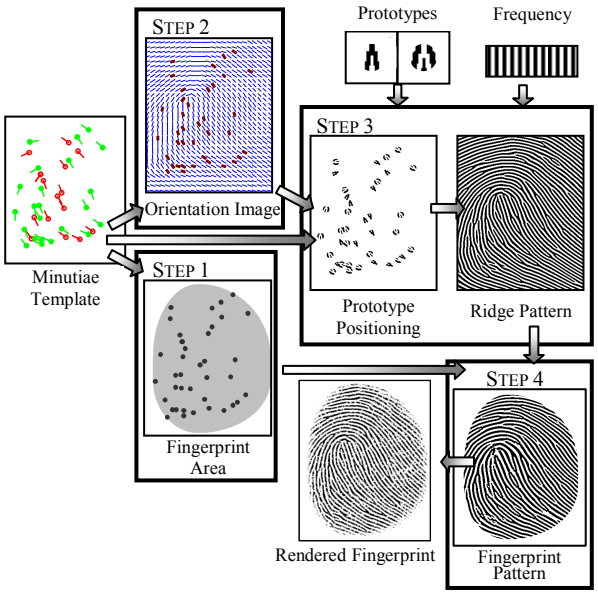

Figure 1: Fingerprint image reconstruction process from the minutiae template.

The reconstruction approach [2] can be summarized by the four steps depicted in Fig. 1: 1) the estimation of the fingerprint area, 2) the estimation of the orientation image, 3) the fingerprint pattern generation, and 4) the final rendering. The second step is not executed in case of ORIMG templates, as the orientation image is known information.

The fingerprint area is estimated according to the elliptical model proposed in [1], minimizing the area that encloses all the minutiae in the template. The orientation image is estimated, starting from the direction of each minutia, optimizing the parameters of the orientation model proposed in [16]. The fingerprint pattern is generated by positioning minutiae prototypes (properly scaled and rotated) on an empty image and iteratively growing the pattern, starting from the orientation image and a given ridge-line frequency. The pattern growing step iteratively modifies the image by applying, at each pixel, a Gabor filter adjusted according to the local frequency and orientation, until the whole image has been covered [2]. Finally a rendering step is performed to make the pattern more realistic.

The fake fingertip creation (Fig. 2) from the fingerprint reconstructed image, is similar to the non-cooperative method described in [13]. First the grayscale of the fingerprint image is inverted, then the inverted image is printed on a slide which will serve as a mask to create a Printed Circuit Board (PCB), where the circuit lines are the valleys of the original fingerprint. The PCB is then covered with a mixture of modeling silicone and a catalyst which reacts with the silicone turning it into a consistent state after a few minutes. When the mixture hardens, it is detached from the PCB and finally the fake fingerprint is cut out from the spare material.

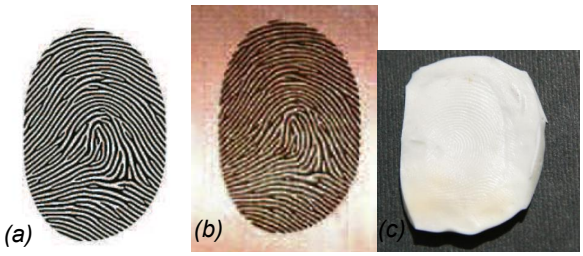

Figure 2: Reconstructed fingerprint image (*a*), fingerprint printed on the PCB (*b*), fake silicon fingertip (*c*).

3. Experimental results

This section reports a preliminary experiment aimed at evaluating the feasibility of a direct attack performed using fake fingertips generated with the method described in the previous section. To this purpose, ten templates (obtained from FVC2002 DB1 fingerprints [4]) have been randomly selected among those that allowed a good image reconstruction in [2]. The rationale behind this choice is to assess how the success chances of an indirect attack are modified when it is transformed into a direct one using fake fingerprints generated from the reconstructed images. Hence, as a first experiment, we decided to study the cases where the reconstructed images could lead to a very successful indirect attack, so that any effect of the fake fingertip creation and acquisition could be easily noticed.

For each template class (MINTYPE and ORIMG), two different rendering types have been evaluated: without noise (BIN), and with noise (REN). The resulting four simulations have been carried out against one of the best commercial fingerprint matchers participating in FVC2002 [4]. In each simulation, three images per template have been reconstructed considering ridge-line periods of 7, 8, and 9 pixels, respectively (Fig. 3).

Figure 3: A fingerprint and all the images reconstructed from its template in the various experiments. From top to bottom: MINTYPE-BIN, MINTYPE-REN, ORIMG-BIN, and ORIMG-REN. From left to right: ridge-line period = 7, 8, 9 pixels.

These images have been used both to simulate indirect attacks and as a starting point to make fake fingertips for the direct attacks.

As in [2], an attack has been considered successful if at least one of the three images (or fingertips in case of direct attack) obtained a matching score higher than the operating threshold. Five different thresholds have been considered (see table 1).

Table 1: The five operating points evaluated: the top row corresponds to the minimum FNMR for FMR=0%; the bottom row is the highest security level considered. All the thresholds have been estimated on the whole FVC2002 DB1 dataset.

Threshold	FMR	FNMR
0.05	0%	0.86%
0.07	0%	1%
0.13	0%	2%
0.30	0%	5%
0.32	0%	10%

Fig. 4 reports the average matching score for indirect and direct attacks in the four cases. It is worth noting that the process of fake fingertip creation and its acquisition through a fingerprint scanner do not seem to noticeably affect the matching score.

Table 2 reports, for each template type, each rendering, and each attack type, the percentage of successful attacks at the five different operating thresholds. From the analysis of the results, the following observations may be made.

- If the local ridge-line orientations are available in the template, the success chances of both direct and indirect attacks are clearly higher; this confirms the findings reported in [2].
- Adding noise to the image rendering step can decrease the success rates of the attacks. While adding noise in the images used for an indirect attack may be a valid attacking strategy to prevent from rejecting the images by simply detecting the absence of noise [2], in case of a direct attack some noise is produced in any case during the acquisition of the fake fingertips.
- If the image reconstruction process has been effective and the fake fingertip creation is carefully performed, transforming an indirect attack into a direct attack does not significantly decrease the success chances of the attack.

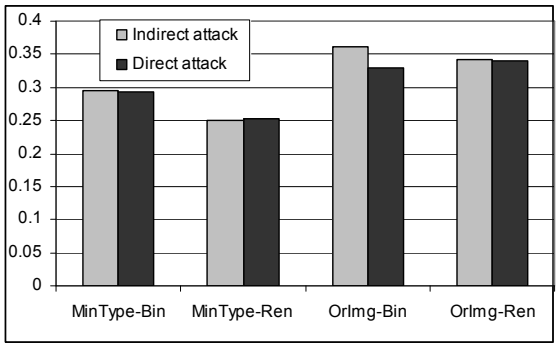

Figure 4: Average matching scores in the four experiments, for both indirect and direct attacks.

Table 2: Percentage of successful attacks in the various experiments, for the five operating thresholds considered. The column headers report the genuine acceptance rate (1-FNMR) to allow an easy comparison with the successful attack rates.

			1-FNMR (%)				
Hypothesis	Render	Attack	99.14	99	98	95	90
MINTYPE	BIN	IND	100	100	80	80	60
		DIR	100	100	80	70	50
	REN	IND	100	100	90	40	30
		DIR	100	90	90	60	30
ORIMG	BIN	IND	100	100	100	90	90
		DIR	100	100	100	80	70
	REN	IND	100	100	100	80	70
		DIR	100	100	100	80	70

5. Conclusions

This work discussed the possibility of performing a direct attack by presenting to the acquisition sensor, a fake fingertip created from an image reconstructed from a minutiae template. We believe this security threat is extremely relevant to recent applications, such as the PIV program [12] or the ILO Seafarers' Identity Document [6], where non-encrypted ISO templates are used.

Although only preliminary results are available at the time this paper is being written, our experiments clearly demonstrate that a direct attack can be successfully carried out against a state-of-the-art recognition system, provided that the image reconstruction process is accurate and that the fake fingertip creation is carefully performed. It has also been shown that orientation information can help to increase the success rate of the attacks.

In order to overcome this type of attacks template protection schemes may be used [8]. In particular, two main strategies can be followed, (*i*) templates can be encrypted by combining them with a random token, performing the matching in the encrypted domain (e.g., Fuzzy Vault [11] and Helper Data System [3]), or (*ii*) a matcher-independent cancelable biometrics approach can be followed [14], generating revocable templates by applying a custom hard-to-invert transformation to the minutiae templates.

Acknowledgements

This work has been supported by the Spanish MDE, the BioSecure NoE and the TEC2006-13141-C03-03 project of the MCYT. J. G. is supported by a FPU Fellowship from the Spanish MEC. J. F. is supported by a Marie Curie Fellowship from the EC.

References

[1] R. Cappelli, "Synthetic fingerprint generation", in D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.

[2] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, pp. 1489–1503, 2007.

[3] M. R. Freire, J. Fierrez and J. Ortega-Garcia, "Dynamic signature verification with template protection using helper data", in *Proc. IEEE ICASSP*, 2008

[4] FVC2002 web site: http://bias.csr.unibo.it/fvc2002.

[5] J. Galbally, J. Fierrez, *et al.*, "On the vulnerability of fingerprint verification systems to fake fingerprint attacks," in *Proc. IEEE ICCST*, 2006, pp. 130–136.

[6] ILO SID-0002, "Finger Minutiae-Based Biometric Profile for Seafarers' Identity Documents", International Labour Organization, 2006.

[7] ISO/IEC 19794-2:2005, Information technology - Biometric data interchange formats - Part 2: Finger minutiae data.

[8] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", *EURASIP Journal on Advances in Signal Processing*, January 2008.

[9] D. Maio, D. Maltoni, *et al.*, "FVC2002: Second Fingerprint Verification Competition", in *Proc. 16th ICPR*, Québec City, vol.3, pp.811-814, 2002.

[10] D. Maltoni, D. Maio, *et al.*, *Handbook of Fingerprint Recognition*, Springer, 2003.

[11] K. Nandakumar, A. K. Jain, and S. Pankanti "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Trans. Information Forensics and Security*, vol.2, no.4, pp.744-757, 2007

[12] NIST Special Publication 800-76, "Biometric Data Specification for Personal Identity Verification", February 2005.

[13] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Proc. IFIP*, 2000, pp. 289–303.

[14] N. K. Ratha, S. Chikkerur, *et al*, "Generating Cancelable Fingerprint Templates," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol.29, no.4, pp.561-572, 2007

[15] U. Uludag and A.K. Jain, "Attacks on biometric systems: a case study in fingerprints", in *Proc. of SPIE*, Volume 5306, 2004, pp. 622-633.

[16] P. Vizcaya, L. Gerhardt, "A nonlinear orientation model for global description of fingerprints", *Pattern Recognition*, 29(7): 1221-1231, 1996.