

On the Generation of Synthetic Fingerprint Alterations

Serena Papi,¹ Matteo Ferrara,² Davide Maltoni² and Alexandre Anthonioz³

Abstract: In this paper we propose some techniques to generate synthetic altered fingerprints and prove the utility of the generated datasets for developing, tuning and evaluating algorithms for altered fingerprint detection/matching. Due to the lack of public databases of altered fingerprints the generation tool proposed (and made freely available) can be a valid instrument to boost research on these challenging problems.

Keywords: altered fingerprints, synthetic alterations, obliteration, z-cut, central rotation.

1 Introduction

In the recent years automatic fingerprint recognition systems are being increasingly used for border and immigration control. With the clear intent of deceiving fingerprint-based identification a subject can produce intentional alterations to his/her fingerprints: if a fingerprint pattern is severely damaged the chance of finding the corresponding pre-altered sample in an AFIS greatly diminishes [YZJ12].

This problem can be tackled in two different ways:

- developing algorithms to detect if a fingerprint pattern has been altered;
- making AFIS capable of matching altered fingerprints (live sample) against pre-altered sample (in the database).

Some research works have been recently devoted to fingerprint alterations, but the problem still remains open due to the difficulty to provide effective solutions.

In [YFJ12], Jain et al. showed that the standard NFIQ approach

[TWW04] does not allow to detect fingerprint alterations and proposed a new approach based on the analysis of orientation discontinuity and minutiae distribution. Another approach for altered fingerprint detection was proposed in [An13] where FFT enhancement is applied for ridge discontinuity analysis and adaptive average filtering/thresholding for scar detection.

A first contribution on matching altered fingerprints comes from [YZJ12] whose authors first studied the capability of commercial fingerprint recognition systems to match

¹ CIRI ICT – Università di Bologna, Via Rasi e Spinelli 146, 47521 Cesena – Italy

² Department of Engineering and Computer Science, University of Bologna, Via Sacchi 3, 47521 Cesena, Italy

³ Ecole des Sciences Criminelles, University of Lousanne, Bâtiment Batochime, 1015 Lausanne - Switzerland

altered fingerprints versus the corresponding pre-altered ones by removing spurious minutiae in the altered region and then proposed an approach for restoring minutiae structure for the Z-cut alterations.

The development of specific solutions for detection/matching of altered fingerprints is very critical due to the lack of public databases containing altered fingerprints and the corresponding pre-altered versions. At today, only police agencies or research groups working together with police agencies have access to altered fingerprint datasets under strict confidentiality agreements, thus limiting the number of scientific contributions to this difficult problem.

Synthetic fingerprint generation proved to be a useful instrument to evaluate/improve fingerprint recognition systems [An13]. Therefore, one possibility to circumvent the lack of available data is generating synthetic altered fingerprints. A first attempt to model fingerprint alterations was made in [Pe12], whose author generated a database of synthetic altered fingerprints; unfortunately this database is currently not available.

In this paper we present an approach for generating synthetic altered fingerprints. We model three of the most frequent alterations, namely obliteration by burning, distortion by central rotation and by Z-cut. The modeling approaches proposed in [Pe12] have been improved in order to obtain more realistic alterations including scars and transitions between native and altered regions and by designing more realistic alteration shapes.

The software tool developed for generating altered fingerprints is made freely available at [SAFG16]. The generation is controlled by a number of parameters and can be performed in batch-mode starting from a given dataset of fingerprints. In particular, the tool allows to generate datasets with alterations of different difficulty levels and to focus on a specific type of alteration or on a mix of different alterations. For more details the reader should refer to the web site page [SAFG16].

From a visual analysis of generated altered fingerprints (see Fig. 2 for some examples) it is quite evident that the generated samples are not visually very realistic; however, at this stage, our scope is not the image realism but the sample utility for the development/tuning of algorithms.

To validate the utility of generated altered fingerprints we show that a fingerprint matching algorithm (MCC [MSW16],[CFM10]) tuned on a synthetic dataset improves its accuracy also on a real dataset of altered fingerprints (not available at tuning time).

The rest of the paper is organized as follows: in Section 2 the problem of fingerprints alteration is presented in more details. In Section 3 we describe the generation process and provide some examples of generated patterns while in Section 4 we show how altered vs pre-altered fingerprints matching can be improved by tuning an algorithm on synthetic samples. Finally, in Section 5 we discuss possible applications and draw some conclusions.

2 Fingerprint alterations

The problem of fingerprints alteration, also known as fingerprint obfuscation, refers to the intentional effort of a person of hiding his/her identity by permanently or temporarily altering ridge patterns [YFJ12]. Usually the alterations are classified into three main categories based on the changes made to the ridge patterns: obliteration, distortion and imitation [YFJ12].

The problem of altered fingerprints was handled by Samischenko, in [An13], where a collection of altered papilla patterns are reported.

The most frequent way to obfuscate the ridge patterns is the obliteration where the pattern is modified by dermal abrasion, burning or using chemical factors. Some dermal diseases can also cause severe alterations of the fingerprint. This kind of alteration, which is easily achievable without any surgery, produces a "granular effect" which completely deletes the ridge patterns (see examples in [An13]).

In surgery-based distortion parts of the skin are cut and plant out at different (unnatural) positions. Usually the local ridge/valley structure remains unaltered while the global structure is heavily changed. Since this kind of alteration does not change the ridge frequency and width, the image quality doesn't change much and the distorted fingerprints often pass an automatic quality control.

Fingerprint imitation refers to an invasive method to cut out a portion of the fingerprint and i) stitching up the adjacent skin (as shown in Figure 11.a of [YFJ12]) or ii) replacing the missing part with skin from other ridged parts (e.g. palms, soles or fingers) as shown in Figure 11.b of [YFJ12].

Table 2 in [YFJ12], reports an exclusive categorization of 4433 altered fingerprints based on the examination of ridge patterns: 89% are obliterated fingerprints, 10% are distorted and only 1% are imitated. Based on this statistic, special care must be taken in modeling obliteration and distortion.

3 Synthetic Altered Fingerprints Generator

We focused on the three most common alterations encountered in real situations: burning obliteration, central rotation and Z-cut [YFJ12].

For each type of alteration, a parametric model is introduced to modify an input (real) fingerprint. After the main pattern modification, some noise (e.g., scars, blurring) is introduced to create a more realistic pattern. The position of the alteration is randomly chosen inside the fingerprint central area to cover the most distinctive fingerprint region, since the alteration intent is to obscure the fingerprint identity. In the following sections the model of each alteration type is described.

3.1 Burning Obliteration

By observing real burned fingerprints, we can note that the ridge pattern is completely destroyed and a granular effect is introduced in the altered region. To simulate this structure we follow the idea proposed in [Pe12] of applying 2D Perlin noise [P85], a kind of gradient type noise often used in computer graphics for texturing. The alteration is produced by adding to the ridge pattern waves with decreasing frequencies and increasing amplitudes.

The obliteration external shape is a 4-sectors ellipse. This shape is generated starting from a circle of center (x_c, y_c) and radius r and computing the length of the four semi axes (a_1, a_2, b_1, b_2) by randomly varying r of a factor $\pm\Delta$.

More in details, let $f(x, y)$ be the input fingerprint, (x_c, y_c) be the center of alteration, and $E(x_c, y_c, a_1, a_2, b_1, b_2)$ be the 4-sector ellipsoidal mask, the obliterated fingerprint f_{obl} is defined as:

$$f_{obl}(x, y) = \begin{cases} f(x, y) & \text{if } (x, y) \notin E \\ (1 - w) * f(x, y) + w * Obl(x, y) & \text{if } (x, y) \in E \end{cases} \quad (1)$$

$$Obl(x, y) = \sum_{i=1}^n 2^i PN(2^{-i}x, 2^{-i}y) \quad (2)$$

where $Obl(x, y)$ is a 2D Perling noise mask, and n is a parameter representing the number of octaves used. In order to merge the original fingerprint and the generated alteration we perform a weighted linear interpolation between $Obl(x, y)$ and $f(x, y)$ according to the distance transform from the ellipsoidal mask. In this way, a smooth transition is created between burned and untouched regions thus making the pattern more realistic.

In the first row of Fig. 2 some examples of synthetic burning obliterations are shown.

3.2 Central Rotation

In Central Rotation a portion of the fingerprint is cut, rotated and pasted again. The cut shape is defined by a 4-sector ellipse E (see previous section) and a simple geometric rotation is performed on the alteration mask E obtaining E_θ . Since E is not circular, we cannot simply replace it with E_θ , but we must limit the paste region to $(E - E_\theta)$. More in details, let $f(x, y)$ be the input fingerprint, E and E_θ ellipsoidal masks, the altered fingerprint is defined as:

$$f_{CR}(x, y) = \begin{cases} f(x, y), & \text{if } (x, y) \notin (E \cup E_\theta) \\ f_\theta(x, y), & \text{if } (x, y) \in E_\theta \\ \max_f \pm \Delta_l, & \text{if } (x, y) \in (E - E_\theta). \end{cases} \quad (3)$$

where f_θ is the input fingerprint rotated of an angle θ around the alteration center (x_c, y_c) , \max_f is maximum value contained in f (representing the background value) and Δ_l is a noise factor.

In the second row of Fig. 2 some examples of central rotation are shown.

3.3 Z-cut

Z-cut is obtained by a z-shaped incision of the skin, the lift of the two triangular strip patches and final sewing up in switched mode. The Z-cut geometry is regulated by the following parameters: the center position (x_c, y_c) , the length L of the three lines of the Z letter, an angle α (see Fig. 1) in the range $[40^\circ, 50^\circ]$, and an angle β representing the cut orientation with respect to the x axis.

Once the coordinates of the four points ABCD composing the Z-cut have been determined (see Fig. 1, left), the three lines defining the Z are replaced by three less regular polygons (whose deviation from the reference lines is randomly defined) (see Fig. 1). The two near-triangular shapes T1 and T2 are then moved, as shown in Fig. 1, obtaining T1' and T2', respectively. To this purpose two affine transforms are used to map the triangle ABC over DBC and the triangle ABD over ACD.

Formally, let $f(x, y)$ be the input fingerprint, and T1 and T2 be the triangular regions, the altered fingerprint is defined as:

$$f_{Zcut}(x, y) = \begin{cases} f(x, y), & \text{if } (x, y) \notin (T1' \cup T2') \\ f_{T1 \rightarrow T1'}(x, y), & \text{if } (x, y) \in T1' \\ f_{T2 \rightarrow T2'}(x, y), & \text{if } (x, y) \in T2'. \end{cases} \quad (4)$$

where $f_{T \rightarrow T'}$ is the affine transformation moving triangle T over T' .

In the last row of Fig. 2 some examples of Z-cut are shown.

4 Experimental Results and Validation

In this section, we introduce some experiments aimed at validating the proposed synthetic generation. In particular, we show how the well-known matching approach MCC SDK 2.0 [MSW16], [CFM10] can be tuned on a synthetic database of altered fingerprint in order to improve its accuracy on a real dataset. Since the MCC SDK 2.0 works directly with minutiae templates, the minutiae extraction algorithm described in [CFM12] has been used to create minutiae templates.

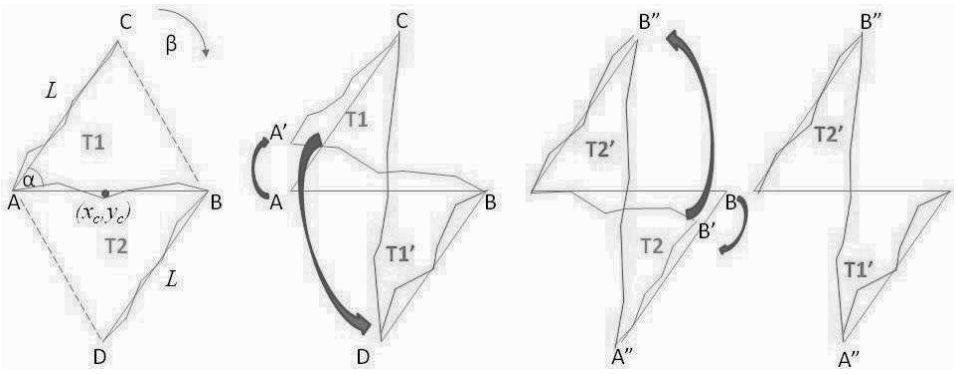


Fig. 1: Scheme of a Z-cut alteration.

4.1 Testing protocol

For each database, each altered fingerprint is compared against:

- the unaltered fingerprints of the same finger to compute the False Non Match Rate (FNMR).
- the unaltered fingerprints of other fingers in the data set, to determine the False Match Rate (FMR).

In case of failure when processing or comparing fingerprints, the corresponding scores are set to zero. The following performance indicators are here considered [M09]:

- Equal-Error-Rate (EER);
- FMR_{100} (the lowest FNMR for $FMR \leq 1\%$).

4.2 UNILDB Database

University of Lousanne has access to a database of real altered fingerprints (UNILDB) containing 1206 rolled fingerprints from 1020 different fingers. The database consists of:

- 1020 unaltered fingerprints from 1020 different fingers (subset U);
- 186 altered fingerprints from 141 different fingers with a mate in U (subset A).

For privacy reasons UNILDB cannot be shared and can be accessed only by Lousanne researchers. In this study we treated it as a “sequestered” dataset not available for algorithm development or tuning, but only to run initial and final version of algorithms.



Fig. 2: Examples of simulated alterations: obliteration (top), central rotation (middle) and z-cut (bottom)

Table 1 reports the NFIQ

[TWW04] distribution on UNILDB. NFIQ (Nist Fingerprint Image Quality) is a five levels quality indicator where ‘1’ means high quality and ‘5’ indicates poor quality. The MCC SDK 2.0 has been tested on UNILDB (by Lousanne personnel) executing 186 genuine and 189534 impostor comparisons. It obtains an EER=19.4% and a

$FMR_{100}=33.9\%$. Note that the accuracy on this difficult task is at least one order of magnitude worse than on typical fingerprint recognition scenario.

NFIQ	UNILDB	Subset U	Subset A
1	755 (63%)	719 (70%)	36 (19%)
2	88 (7%)	82 (8%)	6 (3%)
3	180 (15%)	137 (13%)	43 (23%)
4	146 (12%)	67 (7%)	79 (42%)
5	37 (3%)	15 (1%)	22 (12%)

Table 1: NFIQ distribution on UNILDB

4.3 Synthetic Database

To improve MCC performance on altered fingerprints we generated a synthetically altered database (SYNTHDB) starting from the NIST special database 14 (NISTDB14) [N16]. NISTDB14 has been selected as input database since it contains rolled fingerprints with an NFIQ distribution comparable to UNILDB. NISTDB14 is a public database containing 54000 rolled fingerprints from 27000 different fingers (two impressions per finger). The SYNTHDB consists of:

- a subset SU of 1000 unaltered fingerprints from 1000 different fingers selected from NISTDB4 to match NFIQ distribution of UNILDB subset U;
- a subset SA of 600 synthetically altered fingerprints from 200 different fingers with a mate in SU. In particular for each pre-altered fingerprint one alteration for each of the three types of alterations has been generated (as described in Section 3).

Table 2 reports the NFIQ distribution on SYNTHDB.

The MCC SDK 2.0 has been tested on SYNTHDB by executing 600 genuine and 599400 impostor comparisons. It achieves an EER=12% and a $FMR_{100}=24.2\%$.

NFIQ	SYNTHDB	Subset SU	Subset SA
1	783 (49%)	691 (69%)	92 (15%)
2	132 (8%)	84 (8%)	48 (8%)
3	350 (22%)	141 (14%)	209 (35%)
4	249 (16%)	68 (7%)	181 (30%)
5	86 (5%)	16 (2%)	70 (12%)

Table 2: NFIQ distribution on SYNTHDB

4.4 Minutiae extraction and MCC optimization on SYNTHDB

In order to make the MCC algorithms more effective for altered fingerprint comparison,

its parameters have been optimized on SYNTHDB with the hope to transfer the same performance improvements on UNILDB.

MCC is controlled by several parameters accurately optimized on unaltered fingerprints [MSW16]. Focusing on MCC matching steps, \min_{n_P} , \max_{n_P} , n_{Rel} , δ_θ , and \max_{NR} parameters [CFM10] [CFM12] have been identified as more promising ones and tuned to maximize the recognition accuracy on the SYNTHDB. Beside the above MCC parameters we also established a quality threshold to discard minutiae in very bad quality regions (see Fig. 3). To this purpose we used a local quality measure and optimized the filtering threshold on the SYNTHDB.

The new parameter values are reported in Table 3. Table 5 reports the accuracy indicators obtained on SYNTHDB using the new optimized MCC parameters.

As an additional experiment, we tested the MCC SDK 2.0 and the optimized MCC version on the SYNTHDB subset U of unaltered fingerprints by using the second impression when generating pair attempts. Table 4 reports the results showing that the modified versions perform slightly worse on unaltered fingerprints (for which MCC SDK 2.0 has been optimized). This testifies that specific algorithmic optimization may be necessary to deal with altered fingerprints and that standard (unaltered) fingerprint datasets are useless for this kind of optimization.

MCC parameter	Optimal value on	
	unaltered [MSW16]	altered
$\min_{n_P} - \max_{n_P}$	4-10	4-6
n_{Rel}	2	7
δ_θ	$\frac{3}{4}\pi$	$\frac{5}{6}\pi$
\max_{NR}	50	100

Table 3: Original and modified MCC parameters

Minutiae Extractor Algorithm	MCC	EER %	FMR100 %
Original	Original	1.0	1.0
Modified	Modified	2.0	2.5

Table 4: Accuracy of the original and modified MCC method on the SYNTHDB subset U.

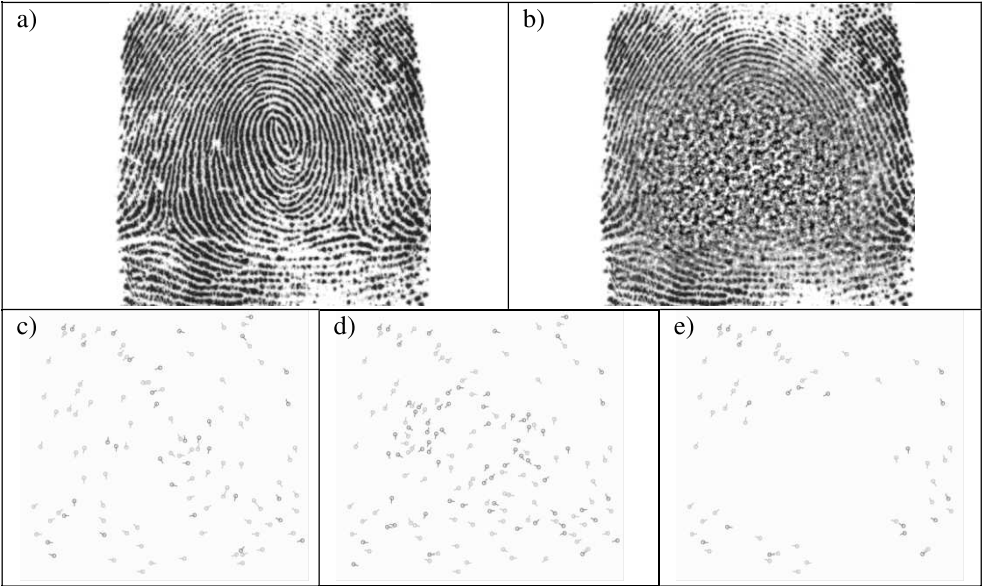


Fig. 3: Several false minutiae are typically located in the altered region, especially on obliterated fingerprints. An example is here reported: a) original fingerprint and c) its minutiae obtained without filtering; b) the synthetically altered fingerprint and d) its minutiae obtained without filtering and e) with quality-based filtering.

4.5 Results on UNILDB

To evaluate if the improvement achieved on the synthetically altered fingerprints can be transferred to real altered fingerprints, the modified MCC SDK has been tested on the UNILDB (see Table 5). An improvement of about 3% has been obtained in terms of both EER and FMR100.

Minutiae Extractor Algorithm	MCC	SYNTHDB		UNILDB	
		EER %	FMR100 %	EER %	FMR100 %
Original	Original	12	24.2	19.4	33.9
Modified	Modified	10.3	19.6	16.1	30.6

Table 5: Accuracy of the original and modified MCC on SYNTHDB and UNILDB.

5 Conclusions

In this work we propose synthetic altered fingerprints as a useful instrument for training and tuning algorithms for altered fingerprint detection and matching, which at today still remain very challenging problems. Even though the alterations generated often appear unrealistic at the human eye we proved their utility in a practical application.

As a future work we intend to improve some of the current generation steps and to model other classes of alterations.

Acknowledgment

The work leading to these results has received funding from the European Community's Seventh Framework Programme (FP7) under grant agreement n° 312792 , [IP16].

References

- [An13] Anoop T. R. Detection of Fingerprint Alteration Using Scars, Minutiae Density and Ridge Discontinuity, *International Journal of Scientific & Engineering Research*, Volume 4, Issue 8, August 2013
- [CFM10] Cappelli R., Ferrara M. and Maltoni D., Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128-2141, Dec. 2010. doi: 10.1109/TPAMI.2010.52
- [CFM12] Cappelli R., Ferrara M. and Maio D., A Fast and Accurate Palmprint Recognition System based on Minutiae, *IEEE Transactions on Systems, Man and Cybernetics - Part B*, vol.42, no.3, pp.956-962, June 2012
- [CMM02] Cappelli R., Maio D., Maltoni D., Synthetic fingerprint-database generation (2002) *Proceedings - International Conference on Pattern Recognition*, 16 (3), pp. 744-747.
- [IP16] Ingress Project web site. <http://www.ingress-project.eu>.
- [M09] Maltoni D., et al., *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.
- [MSW16] MCC SDK Web Site. <http://biolab.csr.unibo.it/mccsdk.html>, June 2016
- [N16] NIST's website at <http://www.nist.gov/srd/nistsd4.cfm>, June 2016
- [P85] Perlin K., An image synthesizer, *Computer Graphics*, vol. 19, no. 3, pp. 287-296, 1985.

- [Pe12] Petrovici A., Simulating alteration on fingerprint images, Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2012 IEEE Workshop on. IEEE, 2012.
- [Sa01] Samischenko S.S., Atlas of the unusual papilla patterns/Atlas neobychnykh papilliarnykh uzorov. (2001).
- [SAFG16] Synthetic Altered Fingerprint Generator Web Site. <http://biolab.csr.unibo.it/strange.html>, July 2016
- [TWW04] Tabassi E., Wilson C.L., and Watson C.I., *Fingerprint Image Quality*, 2004, NIST.
- [YFJ12] Yoon S., Feng J. & Jain A. K., Altered fingerprints: Analysis and detection, IEEE transactions on pattern analysis and machine intelligence, 34(3), 451-464, (2012).
- [YZJ12] Yoon S., Zhao Q., and Jain A.K., On matching altered fingerprints, Biometrics (ICB), 2012 5th IAPR International Conference on. IEEE, 2012.