Improving Fingerprint Alteration Detection

Carsten Gottschlich,* Anna Mikaelyan,† Martin Aastrup Olsen,‡ Josef Bigun,† and Christoph Busch‡
*Institute for Mathematical Stochastics, University of Goettingen, Goldschmidtstr. 7,
37077 Göttingen, Germany. Email: gottschlich@math.uni-goettingen.de
†School of Embedded and Intelligent Systems, Halmstad University,
Halmstad, Sweden S-301 18. Email: {anna.mikaelyan,josef.bigun}@hh.se
‡Norwegian Biometrics Laboratory, Gjøvik University College, Teknologiveien 22,
2815 Gjøvik, Norway. Email: {martin.olsen,christoph.busch}@hig.no

***Abstract*—Fingerprint alteration is a type of presentation attack in which the attacker strives to avoid identification, e.g. at border control or in forensic investigations. As a countermeasure, fingerprint alteration detection aims to automatically discover the occurrence of such attacks by classifying fingerprint images as 'normal' or 'altered'. In this paper, we propose four new features for improving the performance of fingerprint alteration detection modules. We evaluate the usefulness of these features on a benchmark and compare them to four existing features from the literature.**

I. Introduction

In the last five years fingerprint recognition as a well established biometric method has demonstrated its potential to construct large scale Automated Fingerprint Identification Systems (AFIS). The Unique Identification Authority of India has already granted an unique *AADHAAR* number to more than 700 million citizens. The system is designed to provide biometric access to services such as financial transactions and will eventually support 1.2 billion enrollees [1]. In 2011 the European Visa Information System (VIS) was implemented and became operational for all countries in the Schengen area as a distributed system [2]. Again this system will scale up to several hundred million enrollees. The purpose of the VIS is to control during the visa application process that the applicant has no criminal track record and also to verify at the border that the visa holder is eventually the same subject as the one who received the visa at the embassy. While the biometric performance of these systems is impressive and de-duplication can be conducted at low error rates, system operators must consider that there will be a certain fraction of individuals who will try to avoid detection. In both scenarios an individual will not be enroled in the system, if the biometric probe sample captured from the individual matches with a biometric reference already registered in a database, or *watch-list*. Consequently, for negative biometric claims a situation can arise where an individual will alter his fingerprint patterns thus minimizing the chance of detection. Detecting altered fingerprints is a relevant task in border control scenarios, identity management applications relying on a one-to-one relationship between an individual and identification number and in forensic investigations. Criminals or certain other individuals might want to avoid being identified in a watch list or in a database of a law enforcement agency and thus they alter their fingerprint pattern temporarily or permanently. Blacklisted individuals can alter their fingerprint patterns by abrading, cutting or burning their fingerprints. Dedicated surgeries using a Z-shaped cut have been developed, to switch partial skin areas of the fingerprint pattern and consequently render fingerprint comparison algorithms helpless. Fingerprint alterations are a type of presentation attack [4], [5] on biometric systems. These attacks are known as a security risk since 1934, when the murderer John Dillinger tried to avoid identification and burned his fingerprints for this purpose [3]. Around the same time the bank robber Gus Winkler changed the fingerprint pattern of his left middle finger intentionally from *whorl* to *loop* with the aim of confusing identification [3] as illustrated in Figure 1.

Fig. 1. Fingerprint alteration example. Gus Winkler changed in 1933 his left middle finger intentionally from *whorl* to *loop* with the aim of confusing identification. Image source: [3].

However, while the security risk associated with altered fingerprints has been known for a long time, the problem has received little attention from the research community so far. To some degree, this can be explained by the lack of publicly available databases. Realistic data sets to verify the efficiency of alteration detection methods can only be composed through long-term collection by forensic agencies. Only a small number of alteration detection approaches have been proposed so far. In 2010 Petrovici and Lazar have suggested to analyze the reliability of the orientation field as an indicator for alterations [6]. Due to lack of testing data, the method has not been thoroughly evaluated. Yoon and Jain proposed a method that seeks anomalies in the orientation field and features minutia distributions, which are increasing in the presence of scars [7]. The authors were the first to test their method though on a non-public governmental database of several thousand altered fingerprints and reported a correct detection rate of 66% at a false positive rate of 0.3% [7]. Recently Ellingsgaard *et*

Fig. 2. Examples of two unaltered (left, image source: FVC2004) and three altered (right, image source: NIST SD14) fingerprints [8].

al. proposed a method based on the analysis of anomalies in minutia orientations and the fingerprint ridge structure caused by scarred regions [8], which was evaluated on a much smaller semi-public dataset consisting of 116 altered fingerprints.

II. Proposed Method

All fingerprint images have been preprocessed using the factorized directional bandpass (FDB) method [9]. First, the region of interest (ROI) has been estimated by the FDB method and next, images have been automatically adjusted by removing all rows and all columns which contain only background pixels. A visual inspection has been performed to ensure that the automatic preprocessing by the FDB method lead to proper ROIs for all images. Next, we describe four features which we propose for improving fingerprint alteration detection.

A. Proposed Features

DOFTS Mutilation of ridge pattern is one of the main properties of altered fingerprints and therefore, it is natural to use a feature which describes ridge information for alteration detection. We suggest as feature essentially a difference of orientation maps obtained with the complex version of the Structure Tensor [10]. This is represented as a complex vector which is similar to ordinary structure tensor but decomposes the image into two meaningful scalars, one being (complex) orientation and the other being (real) contrast energy used in estimation

$$ST = \begin{pmatrix} I_{20} \\ I_{11} \end{pmatrix} = \begin{pmatrix} \Gamma^{\{0,\sigma_{out}^2\}} * (\Gamma^{\{1,\sigma_{in}^2\}} * f)^2 \\ \Gamma^{\{0,\sigma_{out}^2\}} * |\Gamma^{\{1,\sigma_{in}^2\}} * f|^2 \end{pmatrix} \quad (1)$$

with $\Gamma^{\{n,\sigma^2\}}$ being an n-th symmetry derivative of a Gaussian and f being an image. The parameters σ_{in} and σ_{out} define the inner and the outer scales of the structure tensor.

The contrast energy I_{11} is used to normalize the orientation estimations $I_{20}^L = I_{20}/I_{11}$, with $|I_{20}^L| \leq 1$. These orientation maps are dense and complex valued. It is important to note, that the angular part of the complex valued I_{20}^L is twice the (gradient) direction angle eliminating discontinuities when representing the direction of a line.

Recently, a frequency map estimation has been suggested [12]. In combination with orientation maps above it is used to enhance the image and then reestimate both the orientation and the frequency maps iteratively. This improves the estimated orientation maps. At each iteration a different I_{20}^L is obtained, called $I_{20}^{L(1)}$, $I_{20}^{L(2)}$, etc. Each iteration smooths the orientation map non-linearly. Here we have used 2 iterations and the difference of orientations $\angle I_{20}^{L(2)} - \angle I_{20}^{L(1)}$ has been used as a feature to detect altered fingerprints.

The $I_{20}^{L(1)}$ and $I_{20}^{L(2)}$ have different inner scales through which authentic fingerprint regions obtain similar values and get suppressed in difference computations (similar to e.g. [11]) whereas the altered regions do not. We call the feature Differentials of Orientation Fields by Tensors in Scale (DOFTS).

HIG Histograms of invariant gradients (HIG) [13] also take the orientation field into account and image gradient directions are computed relative to the local orientation. For normal fingerprints, the majority of gradients form an angle of approximately 90 degrees with the local orientation. Alterations of the fingerprint ridge structure change the image gradients in the altered regions and histograms of invariant gradients aim to capture these changes. The HIG descriptor is computed as follows.

First, we compute image gradients for each foreground pixel using the Sobel operator. Second, we estimate the local orientation by averaging squared gradients in window of size 41 pixels. This corresponds to a coarse approximation of I_{20}^L. Third, we obtain an invariant gradient representation by computing the unsigned gradient direction relative to the estimated local orientation. Gradients are sorted into bins based on the relative gradient direction by adding gradient magnitudes to the corresponding bins. Finally, we perform L2-normalization on the histogram. In doing so, we obtain a single HIG descriptor with 180 bins for each fingerprint image.

COH Additionally, we propose the coherence (COH) of gradients as a feature for alteration detection. The coherence measures to what degree the squared gradients in a local neighborhood have a similar orientation. A high similarity of orientations corresponds to a high coherence which is typical for good quality regions in natural fingerprints. Alterations as depicted in Figure 1 and 2 cause areas of very low coherence in the altered regions.

The previously computed image gradients by the Sobel operator are reused for calculating the local coherence of gradients as described in [14]. More precisely, gradients are weighted by a 2D-Gaussian with $\sigma = 8$ in a window of size 33 pixels. The whole foreground image is divided into 3×3 cells, and for each cell, a histogram with 21 equidistant bins (covering the interval of coherence values from 0 to 1) is extracted.

Abbreviation	Description
MDA	Minutia distribution analysis [7]
OFA	Orientation field analysis [7]
SPDA	Singular point density analysis [8]
MOA	Minutia orientation analysis [8]
DOFTS	Differentials of orientation fields by tensors in scale [12]
HIG	Histograms of invariant gradients [13]
COH	Coherence of gradients [14]
MH	Minutiae Histograms [15]

TABLE I. OVERVIEW OVER THE FEATURES APPLIED FOR ALTERATION DETECTION. THE FIRST FOUR FEATURES ARE KNOWN FROM THE LITERATURE, THE LAST FOUR FEATURES ARE NEW IN THE CONTEXT OF FINGERPRINT ALTERATION DETECTION.

MH Minutiae histograms (MH) [15] have been introduced to differentiate between images of real fingers and artificially generated fingerprint images using the earth mover's distance [16]. For each fingerprint, we compute a 10×10 minutiae histogram (MH) [15]. All minutiae pairs are sorted into one of 10 bins for the Euclidean distance between minutiae locations (0 to 200 pixels, first dimension) and one of 10 bins for the directional difference between minutiae directions (0 to $180°$, second dimension). Finally, the sum of all entries is normalized to a total mass of 1.

B. Alteration Score

DOFTS and COH output images which are divided into 3×3 cells. For each cell, we compute a histogram with 21 equidistant bins. In summary, feature vector sizes are 189 for DOFTS and COH, 180 for HIG and 100 for MH.

Experiments have been performed using LIBSVM [17] with a linear kernel ($C = 1$) and regression to obtain an alteration score between 0 and 1 for all features and all images, where 0 corresponds to natural fingerprints and 1 to altered fingerprints.

III. PAD METRICS, DATABASE ANS RESULTS

International standards to measure biometric performance of fingerprint recognition are well established with ISO/IEC 19795-1 [18] and define in which way algorithm errors such as false-match-rate (FMR) and false-non-match-rate (FNMR) must be reported.

Unfortunately, for testing presentation attack detection such established concepts did not exist in the past. ISO/IEC has recently started to work on a standard covering presentation attack detection and metrics to report the efficiency of fingerprint alteration detection methods to counter subversive attacks. The standardization project ISO/IEC 30107 *Biometric presentation attack detection* is providing a harmonized definition of terms related to attack techniques [5], as well as testing methods that can measure robustness against said attacks [19].

In analogy to biometric performance the metrics specified for alteration detection are given by the false-positive *normal presentation classification error rate* (NPCER), which is defined as proportion of normal presentations incorrectly classified as attack presentations, and on the other hand by the false-negative *attack presentation classification error rate* (APCER), which is defined as proportion of attack presentations incorrectly classified as normal presentations. A challenge in this definition is that unlike for biometric performance testing a large corpus of testing samples can not be assumed to be available.

In this work we have used the same limited dataset from [8], however in order to avoid any impact of background area on the performance, all images were pre-segmented by the FDB method [9]. In total 116 altered fingerprint images and 180 unaltered, normal fingerprint images were used. In order to cope with the limited size of this dataset we performed cross-validation by splitting the dataset 100 times into training set and test set. Each training set comprises 80 altered and 80 unaltered images, which are chosen independently and uniformly at random. The remaining 36 altered and 100 unaltered images build the test set.

A comparison of the alteration detection performance for the four existing and the four novel features in terms of detection error trade-off (DET) curves is depicted in Figure 3. Of special interest for practical applications in a border control scenario is the comparison of performance at the left margin of Figure 3. Low false alarm rates (NPCERs) are a desirable property for a fingerprint alteration detection module, because higher NPCERs would entail a larger number of manual inspections of fingerprints by human experts resulting in higher costs for personnel or a decreased throughput speed of border crossings.

IV. DISCUSSION AND CONCLUSION

The four best performing features so far are OFA [7], DOFTS [12], COH [14] and SPDA [8]. The two best performing features OFA and DOFTS are based on differences between orientation fields. The coherence of gradients (COH) and singular point density analysis (SPDA) are also connected to the orientation field, because singular points are estimated from OFs. We conclude that orientation fields contain a high amount of information which is useful for detecting altered fingerprints. An advantage of the HIG descriptor [13] is that it can be computed very fast (in a few milliseconds per image) and it contributes to both alteration detection and liveness detection. The three features MDA, MOA and MH use the minutiae template as input. Out of these three, minutiae histograms (MH) [15] performs best at a NPCER of 1%. Minutiae histograms [15] are useful for detecting unnatural minutiae configurations which can be caused by fingerprint alteration or a presentation attack with a synthetically generated fingerprint image.

In summary, we have proposed four new features for fingerprint alteration detection. Two of these are among the three best performing features on the considered benchmark at a NPCER of 1% which is of special relevance for practical applications in border control. As future work we plan to investigate additional features, e.g. ridge frequency maps obtained by the structure tensor [12] or by curved regions [20]. Orientation maps obtained by the structure tensor are complex valued with angular information representing orientation and magnitude defining reliability. In this paper we have utilized the angular information only leaving space for improvement by incorporating the magnitude in future works. Moreover, we plan to explore feature-level or score-level fusion between two or more features. We intend to analyze to which degree

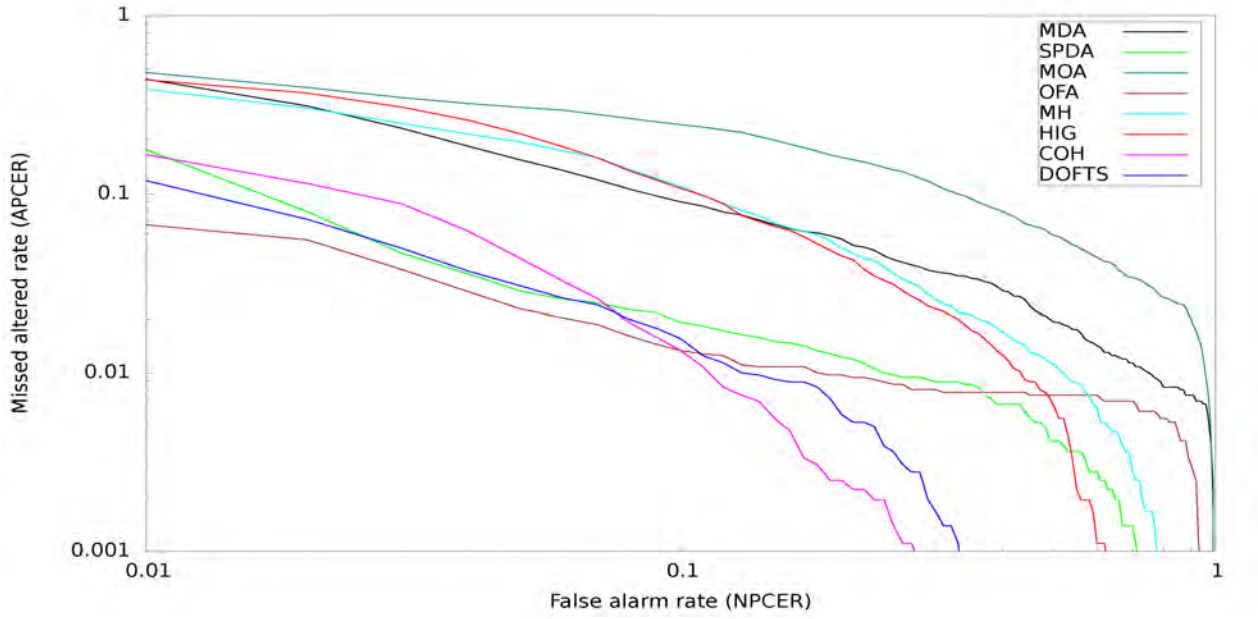

Fig. 3. Detection error trade-off curves comparing the alteration detection performance for the features listed in Table I. Results are averaged APCERs at corresponding NPCERs (from 0% to 100% in steps of 1%) averaged over 100 random splits of the dataset into training and test sets.

features are complementary with simultaneous consideration of potential synergy effects between fingerprint alteration detection and other processing modules e.g. for image enhancement or liveness detection.

ACKNOWLEDGEMENTS

This work is carried out under the funding of the EU-FP7 INGRESS project (Grant No. SEC-2012-312792). C. Gottschlich also acknowledges the support of the Felix-Bernstein-Institute for Mathematical Statistics in the Biosciences and the Niedersachsen Vorab of the Volkswagen Foundation.

REFERENCES

[1] UIDAI, "Role of biometric technology in aadhaar enrollment," Unique Identification Authority of India, New Dehli, India, Tech. Rep., Jan. 2012.

[2] European Council, "Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)," Jul. 2008.

[3] H. Cummins, "Attempts to alter and obliterate finger-prints," *Journal of Criminal Law and Criminology*, vol. 25, pp. 982–991, May 1935.

[4] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, Dec. 2014.

[5] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC DIS 30107-1. Information Technology - Biometric presentation attack detection - Part 1: Framework*, International Organization for Standardization, 2015.

[6] A. Petrovici and C. Lazar, "Identifying fingerprint alteration using the reliability map of the orientation field," *The Annals of the University of Craiova. Series: Automation, Computers, Electronics and Mechatronics*, vol. 7(34), no. 1, pp. 45–52, 2010.

[7] S. Yoon, J. Feng, and A. Jain, "Altered fingerprints: Analysis and detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 3, pp. 451–464, Mar. 2012.

[8] J. Ellingsgaard, C. Sousedik, and C. Busch, "Detecting fingerprint alterations by orientation field and minutiae orientation analysis," in *Proc. IWBF*, Valletta, Malta, Mar. 2014, pp. 1–6.

[9] D. Thai, S. Huckemann, and C. Gottschlich, "Filter design and performance evaluation for fingerprint image segmentation," *arXiv:1501.02113 [cs.CV]*, Jan. 2015.

[10] J. Bigun, *Vision with direction*. Berlin, Germany: Springer, 2006.

[11] A. Mikaelyan and J. Bigun, "Symmetry assessment by finite expansion: application to forensic fingerprints," in *Proc. BIOSIG*, Darmstadt, Germany, Sep. 2014, pp. 75–86.

[12] J. Bigun and A. Mikaelyan, "Dense frequency maps by structure tensor and logarithmic scale space: application to forensic fingerprints," submitted.

[13] C. Gottschlich, E. Marasco, A. Yang, and B. Cukic, "Fingerprint liveness detection based on histograms of invariant gradients," in *Proc. IJCB*, Clearwater, FL, USA, Sep. 2014, pp. 1–7.

[14] C. Gottschlich and C.-B. Schönlieb, "Oriented diffusion filtering for enhancing low-quality fingerprint images," *IET Biometrics*, vol. 1, no. 2, pp. 105–113, Jun. 2012.

[15] C. Gottschlich and S. Huckemann, "Separating the real from the synthetic: Minutiae histograms as fingerprints of fingerprints," *IET Biometrics*, vol. 3, no. 4, pp. 291–301, Dec. 2014.

[16] C. Gottschlich and D. Schuhmacher, "The shortlist method for fast computation of the earth mover's distance and finding optimal solutions to transportation problems," *PLoS ONE*, vol. 9, no. 10, p. e110214, Oct. 2014.

[17] C.-C. Chang and C.-J. Lin, "LIBSVM : a library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, no. 3, pp. 1–27, Apr. 2011.

[18] ISO/IEC TC JTC1 SC37 Biometrics, *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, International Organization for Standardization and International Electrotechnical Committee, Mar. 2006.

[19] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC CD 30107-3. Information Technology - Biometric presentation attack detection - Part 3: Testing and Reporting*, International Organization for Standardization, 2015.

[20] C. Gottschlich, "Curved-region-based ridge frequency estimation and curved Gabor filters for fingerprint image enhancement," *IEEE Transactions on Image Processing*, vol. 21, no. 4, pp. 2220–2227, Apr. 2012.