Creation of a Public Corpus of Contact-Less Acquired Latent Fingerprints without Privacy Implications

Mario Hildebrandt, Jennifer Sturm, Jana Dittmann, Claus Vielhauer

Creation of a Public Corpus of Contact-Less Acquired Latent Fingerprints without Privacy Implications

Mario Hildebrandt[1], Jennifer Sturm[1], Jana Dittmann[1], Claus Vielhauer[2]

[1]Research Group on Multimedia and Security, Otto-von-Guericke University of Magdeburg, Universitaetsplatz 2, 39106 Magdeburg, Germany
{hildebrandt, sturm, dittmann}@iti.cs.uni-magdeburg.de
[2]Brandenburg University of Applied Sciences, Magdeburger Str. 50, 14770 Brandenburg an der Havel, Germany
vielhauer@fh-brandenburg.de

Abstract. Data sets of biometric or forensic samples are an important basis for evaluations and research. Especially biometric data is considered as personal data, which is protected by privacy regulations. Since the data cannot be altered or revoked, at least in some countries, this poses a challenge because rights must be granted to the data's subject. In particular in Germany and probably in the entire European Union after its reformation of the data protection legislation it is challenging to use such data. Furthermore, with respect to latent fingerprints only very few public data sets exist nowadays. We propose the creation of a public data set without privacy implications consisting of latent fingerprints from artificial fingerprint patterns. On the foundation of a first set of 50 fingerprints on a compact disk surface we report challenges that need to be solved in order to create realistic samples.

Keywords: Forensics, latent fingerprints, public data set, privacy aspects.

1 Extended Abstract

In biometrics and forensics evaluations of new and existing techniques are very important in order to determine error rates especially when such methods are used e.g. for authentication systems or for the analysis of evidence. In forensics the Daubert challenge [1] comprises several factors that can be assessed by a judge prior to admitting evidence in court. Furthermore, researchers need to show that their proposed methods pose an advance in science and technology. Here, public data sets help compareing the evaluation results with each other without any bias. However, especially biometric data need to be considered in most cases as personal data [2]. Thus, it is covered by privacy regulations and data protection acts. Moreover, the possibility of replicating biometric traits or traces can increase the risk for identity theft [5]. Hence, in some legislations, such as in Germany [3], the public usage of biometric data sets is challenging since certain rights must be granted to the person concerned. Furthermore, it is expected that the reform of the European data protection legislation will

strengthen individual rights as well [4], leading to higher barriers in creating and using public biometric data sets. In contrast to similar fields such as biometric systems where biometric data and templates can be transferred and stored in an encrypted or obfuscated manner (e.g. in fingerprint authentication [9]) to ensure privacy, an access to the original raw fingerprint data is necessary for research purposes and various evaluations. Moreover, in forensics an access to the fingerprint image is necessary because the examiner is responsible for a final decision.

We address this challenge by proposing a data set of contact-less acquired printed artificially created latent fingerprints for the evaluation of forensic techniques. In doing so, we want to generate latent fingerprints as realistic as possible while retaining the ability to detect them as motivated by Kiltz et al. [5]. To avoid any privacy implications artificial fingerprint patterns are generated using SFinGe [6] and afterwards printed using a Canon Pixma iP4950 ink-jet printer with the technique of Schwarz [7]. The intention of SFinGe is the creation of fingerprints for the evaluation of biometric systems. For that, it is supported to add noise, distortions and sensor influences. However, in forensics latent fingerprints can be found on various substrates that potentially require the acquisition with different sensors. The printing process ensures that the fingerprint pattern can be applied to a broad variety of such substrates and thus creating realistic conditions for forensic investigations. In our first experiments, the samples are digitized using a Keyence VK-x110 series confocal laser scanning microscope which captures topography and intensity data using a laser and color data by using a CCD camera. Furthermore, a color-intensity image is generated by combining the color data and the laser data. Since this measurement device stores the digitized trace within a proprietary format, we convert the image data for the public database into simple binary objects consisting of an 8 bit header with the width and the height of the data field followed by either a field of 32 bit little endian floating point values for topography and laser intensity data or 32 bit ARGB values for color and color-intensity data. This allows for analyzing the data with various tools. The four binary objects are accompanied with a meta-data file with the sensor and its parameters which are necessary for the interpretation of the data.

In our poster, we show and discuss the challenges of the creation of the data set on the foundation of 50 samples. In particular, the reproducibility of the printing results and the overall realism of the acquired fingerprints need to be further enhanced in order to replace real biometric traces from the human. The reproducibility of the printing results is primarily affected by the reliability of the printing process. Nozzles or the entire print head tend to be clotted [5] since the artificial sweat has different properties than the manufacturer ink. The realism of the printed latent fingerprints trace is also negatively affected by this effect leading to a visible pattern of amino acid dots instead of continuous ridge line impressions. Hence, in order to address those challenges, we propose a work around to enhance the ridge clarity within the digitized data which connects neighboring dots to create continuous ridges. The method applies a hit or miss operator as a first processing step leading to a binarized image of multiple dots of amino acid. In the second step a triangulation is used to connect the dots. A threshold for the maximum distance between dots is applied to avoid connecting dots between different ridges. The result is a binarized fingerprint

pattern similar to the original sample. However, this approach would likely not work on non-smooth or textured surfaces due to the surface noise. Furthermore, such a processing is unsuitable to achieve realistic traces.

For quality measurement, we adapt a correlation based measure from [8] to determine whether the digitized trace and the original pattern are sufficiently similar. It is based on the Pearson product-moment correlation coefficient of the images. However, this requires an exact alignment and scaling of the data.

In future work the reliability of the printing process and the realism of the printed patterns need to be increased in order to create usable data sets for forensic sciences.

Acknowledgement

The work in this paper has been funded in part by the German Federal Ministry of Education and Science (BMBF) through the Research Program under Contract No. FKZ: 13N10818 and FKZ: 13N10816.

References

1. L. Dixon and B. Gill. Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases Since the Daubert Decision. RAND Institute for Civil Justice, 2001. ISBN: 0-8330-3088-4.
2. Article 29 Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies, 2012. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
3. Federal data protection act (BDSG), 2010. [Online]. Available: http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.
4. European Commission. How does the data protection reform strengthen citizens' rights?, 2012. [Online]. Available: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf.
5. S. Kiltz, M. Hildebrandt, J. Dittmann, C. Vielhauer, and C. Kraetzer. Printed fingerprints: a framework and first results towards detection of artificially printed latent fingerprints for forensics. In Image Quality and System Performance VIII, Proceedings of SPIE Vol. 7867, 2011.
6. D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition (Second Edition). Springer, London, 2009.
7. L. Schwarz. An amino acid model for latent fingerprints on porous surfaces. Journal of Forensic Sciences, 54(6):1323{1326, 2009.
8. J. Sturm, M. Hildebrandt, J. Dittmann, and C. Vielhauer. High quality training materials to detect printed fingerprints: Benchmarking three different aquisition sensors producing printing templates. In International Workshop on Biometrics and Forensics (IWBF) 2013, Lisbon, Portugal, 2013.
9. M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva. Privacy-preserving fingercode authentication. In Proceedings of the 12th ACM workshop on Multimedia and security (MM&Sec '10), 231-240. 2010.