Digital Dactyloscopy: A First Design Proposal for a Privacy Preserving Fingerprint Scanning System

Matthias Pocs / Benjamin Stach
Project Group Constitutionally Compatible Technology Design (provet)
Universität Kassel, Germany
{matthias.pocs, benjamin.stach}@uni-kassel.de

Mario Hildebrandt / Stefan Kiltz / Jana Dittmann
Research Group on Multimedia and Security
Otto-von-Guericke University Magdeburg
Magdeburg, Germany
{hildebrandt, kiltz, dittmann}@iti.cs.uni-magdeburg.de

***Abstract*—Biometric technology for crime prevention is emerging. One example is digital contact-less capture of fingerprint traces, which is currently under development. As a first approach we propose the design of a system for securing court evidence. The proposal is based on an evaluation of data formats for the application in future fingerprint scanning systems and is derived from requirements of the German law. Aiming at enhancing privacy, preserving anonymity and protecting against illegitimate "identity change," this proposal shows how to derive technology design proposals from human rights law using a fingerprint scanning system as an example.**

Keywords-privacy and data protection; dactyloscopy; fingerprint scanning system; digital capture; biometric systems; German law on court evidence.

I. INTRODUCTION

Fingerprints are used for decades in forensics to identify that people were present at some point in time at a crime scene or have touched certain items, potentially linking them to a crime. The methods for the acquisition and analysis of traces have not changed significantly over this long period. A major improvement was the introduction of automated fingerprint identification system (AFIS) [1]. This particular system uses an automated identification of potentially matching fingerprints. However, all candidates (usually 15-20) are verified manually by forensic experts. Even with those precautions misidentifications are possible [2].

New acquisition techniques might allow for a non-destructive collection of fingerprint traces with one or multiple sensors in crime prosecution and prevention use-cases [3]. The use of such new techniques can provide more information about a single trace since it can be investigated all over again from different perspectives and using different techniques. This allows for a more thorough investigation by forensic experts and might reduce the risk for misidentifications. However, the application of new sensors and the subsequent investigation of the digitised traces constitute a major change of the generally accepted investigation process of fingerprint traces.

In order to achieve those goals, a first process model for the digital dactyloscopy is introduced in [4]. It is derived from a process model intended for digital forensics because similar precautions must be regarded during the investigation process in digital forensics. The derived process model consists of seven phases: *strategic preparation*, *physical acquisition*, *operational preparation*, *data gathering*, data *investigation*, *data analysis* and *documentation*. The documentation is divided into a *process accompanying documentation* consisting of a detailed record of all performed actions together with all their parameters, and a *final documentation* as a concluding result of the forensic analysis. Additionally, the security aspects *integrity* and *authenticity* [21] of the processed data must be considered and addressed throughout the entire investigation. Since digital data can be copied and transferred easily, the security aspect of *confidentiality* [21] must be retained to preserve the privacy [20]. Furthermore, the anonymity should be preserved by the unlinkability [20] between a trace and the name until a matching reference sample is found. Subsequently, the security aspects non-repudiation [21], e.g., for the chain of custody, and availability [21] might be required for the investigation of fingerprint traces.

In this paper we evaluate various data formats, including the container format for digitised fingerprint traces from Kiertscher et al. [5], a database-centric approach [6] and a data format for multiple data streams for use in digital forensics [7], for their applicability in a future fingerprint scanning system. For that we derive requirements from the German law. Furthermore, we introduce a legal approach as a foundation for our technical design proposal of a future fingerprint scanning system derived from German law principles. This particular technical design proposal is intended to be applicable for the fingerprint acquisition on crime-scenes and in a forensic lab. It aims at enhancing privacy and preserving anonymity. The standard of data privacy is quite strict in Germany from a comparative law point of view. Therefore, any requirement regarding data privacy might be suited as a showcase requirement. Nonetheless, it has to be considered that criminal law proceedings may differ highly in certain national legislation.

This paper is structured as follows: In Section I, we analyse legal aspects of court evidence. Our legal approach is introduced in Section III. We summarise the process model for the digital dactyloscopy and the forensic data formats that are evaluated in this paper in Section IV. We define main technical requirements and introduce our first design approach in Section V. In Section VI, we analyse the suitability of various selected forensic data formats for future fingerprint scanning systems. Finally, we summarise the challenges for a digitised fingerprint analysis and outline future work in Section VII.

 ISBN: 978-1-61208-182-3

II. EVIDENCE IN COURT

In Germany, statutory law and its judicial interpretation governs court proceedings. Evidence is defined as the assessment of facts (of a case) as an established fact by judicial persuasion. German law recognises several principles in criminal proceedings. The principle regarding evidence is particularly the principle of free evaluation of the evidence, which is set out in § 261 Code of Criminal Proceeding (*Strafprozessordnung*).

Besides, the criminal procedure is a strict *inquisitorial system*. This means the court conducts its own investigation and may not rely solely on the facts and evidence presented by the parties. Furthermore, the *Rechtsstaat* principle (best translated as "law-based state" principle) in art. 20 para. 3 Basic Law (*Grundgesetz*) and art. 6 *European Convention on Human Rights* demands the trial to be conducted fairly. Due to the 'fair trial' principle, police and prosecution have to consider both the burdening and the unburdening facts.

A. Significance of Traces of Fingerprints as Evidence

Fingerprints may be used to identify a person. Every person has an individual fingerprint, even identical twins. Thus, traces of fingerprints are significant as evidence. But it is crucial to point out that fingerprints may only be used to link a certain person to a certain place. Digitalisation might add a greater value to fingerprints as evidence in court.

Digitalisation by contactless devices is a non-destructive method to obtain fingerprints. Until now forensic scientists use so called developer to detect contrasts between the ridge patterns and the surface. The developer is usually a powder or even a chemical reagent. Such technologies destroy any potential DNA traces on the particular fingerprint.

Digitalisation might even produce more information than conventional methods. At the moment, forensic scientists are not able to separate overlapping fingerprints or to estimate the age of a fingerprint. Both may be possible by means of digitalisation and is currently under research.

B. Risks of Digitalisation

Digitalisation might bear several risks. These risks might impede the use of digitised fingerprints in court at all. Thus, these risks need to be excluded by technical means.

1) Tampered Evidence: Digital evidence might be tampered with. The risk of tampering is higher by digital means than by analogous ones. The problem is that manipulations can be done even without special knowledge. Furthermore, manipulation might not be detected at all. This also includes unintentional manipulations, e.g., corruption by storage errors. Tampered evidence would be useless in court because it might not be admissible as evidence at all or would be at worst the cause for an unjust ruling.

2) Evidentiary Value: Digitally collected fingerprints must not be handled differently to normal fingerprints. As an example, a dirt smudge cannot be regarded as a precise imprint only on the basis of being collected digitally and a precise imprint needs to be treated as such. Therefore, the information on the quality of the taken imprint needs to be linked tightly to the presented digital image.

C. Enhancing the evidentiary value

Accordingly, if these risks could be excluded, digitalisation would enhance the evidentiary value of fingerprints as evidence in court. Furthermore, digitalisation might even allow more probative facts to be collected.

1) Secured Chain of Custody: A secured chain of custody can exclude any tampering of the evidence. A complete verification and a complete presentability are necessary for this purpose.

2) Integrated Context Data: Context data can additionally give a description of how the fingerprint has been collected by whom, where and when. Also, the age of the imprint might be added as context data. The forensic scientist needs to add the quality of the found imprint. This ensures that all the collected data is bound together. The context data needs to be presentable.

3) Conclusion: For the purpose of evidence, any data of the digitised fingerprint has to be stored in a secured chain of custody. This involves any additional context data, such as location and time of collection or age as well as quality of the imprint. Any context data would enhance the evidentiary value contrary to plain analogous forensic scientists' transcript by including it into the secured chain of custody.

III. LEGAL FRAMEWORK

The German constitutional principle of the *Rechtsstaat* lays down that innocence of persons accused of a crime be assumed until evidence is furnished [8]; this is also enshrined in art. 6 *European Convention on Human Rights*. In relation to data processing one has to comply with the fundamental right to informational self-determination according to art. 2 para. 1 i.c.w. art. 1 para. 1 *Grundgesetz*. This aims at enhancing privacy and preserving anonymity of nonsuspects and protecting them against "identity change."

A. Legal Requirements

Currently fingerprints at crime scenes are manually collected by the police officer in charge of securing evidence. During criminal proceedings the fingerprint as well as the officer's record about securing the fingerprint with his/her signature on that record are furnished as documentary evidence pursuant to §§ 249 ff. *Strafprozessordnung*. The authenticity of the record is proven by means of the officer's testimony to the signature on the record pursuant to §§ 48 ff. *Strafprozessordnung*. For automatic capture of fingerprint traces, this means that it needs to have a solid scientific and technological basis, be applied without error and ensure that the fingerprint traces have a quality suitable for furnishing evidence [9]. Moreover, integrating context data can increase the evidentiary value.

B. Legal Criteria

There are several legal criteria that specify the general legal criteria of scientific and technological basis, error-free application, trace quality and integration of context data.

For establishing the existence of a scientific and technological basis we may put forward several criteria (testing, standards, comprehensibility by experts/judges, and

error rates). Concerning the error rates one has to consider that the fingerprint scanning system does not decide whether or not a fingerprint belongs to a certain person but only digitises the trace of a fingerprint. Deciding on similarity of two fingerprints is not part of it. Nonetheless, there may be errors (wrong choice of surface material, "regions-of-interest," or distinction surface/fingerprint). The significance or the error rate needs to be explored in the future.

Concerning the error-free application of the method the fingerprint scanning system offers an opportunity. This is due to the fact that the fingerprint captures are automated and the method can be applied without error as far as it is automated. One can clarify what processes are automated.

Avoiding error or manipulation is achieved by measures of data security relying on the state of the art [10]. All stages of processing within the scanning system are logged in a secure way [11]. These processes also comprise manual inputs of additional information that is necessary for the evaluation of secured fingerprints. The data must be secured from the time of data capture.

Sophisticated encryption oriented towards the state of the art and secure access should be used [12] [13]. Further the scanning system may be protected using digital watermarks. Watermarks can be reversible or irreversible. As long as the data are not devaluated in a way that the scientific basis does not apply anymore, irreversible watermarks are preferable because they guarantee increased data integrity.

The trace quality relies on the trace and properties of the surface material, which has to be considered when designing the system. One can explore how to collect information about the trace quality by automatic means; this may be a research question for the future. Surface material information is manually entered; also with conventional methods such information needs to be collected [14]. However, it needs to be adapted and defined for the scanning system.

Integrating context data is a new possibility the scanning system offers. Currently the police officer is in charge of proving the time of securing the evidence and place of the crime scene using his/her respective record. With the fingerprint system, the information about time and place could be captured automatically (secured system time/GPS or time/place stamps) in order to rule out confusion of different investigations. In this way the evidentiary value of the captured fingerprint data is increased.

In addition, research promises to determine additional context information about the fingerprint. First the scanning system can determine the age of the fingerprint. The age of such traces is decisive to establish whether or not the trace was left during the criminal activity [15]. Furthermore, the system can separate overlapping fingerprints. Moreover, spoofing the capture device by using artificial fingerprints can be revealed. Such attacks will be more likely in the future if use of biometric systems will increase [16].

IV. STATE OF THE ART

We use the process model for the digital dactyloscopy [4] to describe our concept of a criminal court proved design of a future non-destructive optical fingerprint scanning system. Furthermore, we analyse different data storage formats or concepts as a base for the digitised forensic investigation.

A. Process model for the digital dactyloscopy

The process model for the digital dactyloscopy [4] consists of seven phases. During the first phase *strategic preparation* (SP) potential investigations are prepared. This phase describes procedures and techniques used ahead of a specific incident. Those include the acquisition and installation of sensors, as well as training arrangements for the personnel. Furthermore, a software directory, sample material and aging models should be created and evaluated by benchmarking [17]. Subsequently, guidelines for the physical acquisition should be defined for crime scene investigators to avoid any alteration of fingerprint traces.

The *physical acquisition* (PA) describes the identification and acquisition (e.g., seizure) of physical objects that might contain fingerprint traces. The crime scene investigator should also decide whether the object can be transported to a forensic lab for the acquisition or whether it is better to acquire it directly on the crime scene (e.g., if the object is too large or if the trace might be destroyed during the transport).

The *operational preparation (OP)* describes all processes that are required prior to the digital acquisition. In particular, it includes the choice of the appropriate acquisition sensors and processing methods to achieve the highest possible quality of the digitised trace. Here the results of the strategic preparation will be used.

During the *data gathering* (DG) several actions are performed to acquire the fingerprint traces from a particular object using contact-less sensory equipment. Firstly, the required acquisition parameters and material properties are determined. Secondly, a coarse scan is performed to detect Regions-of-Interest (ROI) that need to be acquired with a detailed scan. Subsequently, each ROI is acquired using high-resolution detailed scans.

The *data investigation* (DI) contains all pre-processing steps prior to the fingerprint ridge pattern analysis. In this phase overlapping fingerprint patterns are separated, the age of each pattern is determined and the visibility of the ridge pattern is enhanced for the manual analysis using pre-processing techniques.

The identification of the fingerprints is performed during the *data analysis (DA)*. It is performed manually with optional machine assistance (e.g., feature extraction and highlighting). The investigation should strictly adhere to current investigation standards: the analysis, comparison, evaluation, and verification (ACE-V) methodology, etc. [1]

Subsequently, the results are summarised in the phase of the *documentation (DO)*. Besides the concluding final documentation a process accompanying documentation contains a detailed log of all performed investigation steps throughout the whole process. This allows for an enhanced comprehensibility of the course of the investigation.

B. Forensic data storage and exchange formats

Various formats for the storage and exchange of forensic traces exist. In this paper we compare the *data format for the interchange of fingerprint, facial & SMT information*

(ANSI/NIST-ITL 1-2000) [18], the *Advanced Forensics Format (AFF4)* [7], a container format for digitised fingerprint traces [5] and a database centric approach for digitised fingerprint traces [6].

The *data format for the interchange of fingerprint, facial & SMT information* (ANSI/NIST-ITL 1-2000) is used for the exchange of fingerprint data for the automated fingerprint identification systems (AFIS) [1]. The design goals for this particular format are *openness*, *non-intrusiveness*, *inter-operability* and *wide usage*. The data format consists of ASCII and Binary data records. Those logical records include transaction information, user-defined descriptive texts, fingerprint images in different resolutions and encodings (e.g., Binary and greyscale), a user defined image, an image of the handwritten signature of the subject and/or the officer, minutiae data, images of latent prints or Common Biometric Exchange Formats Framework (CBEFF) [19] [19] Biometric data records. It supports various image formats for the fingerprint image: uncompressed images, WSQ version 2.0, lossy and lossless JPEG, lossy and lossless JPEG 2000 and PNG. Images can be binary, greyscale or colour data.

The *Advanced Forensics Format 4 (AFF4)* [7] is designed for digital forensics. It is able to store multiple digital traces within a single volume. The data can be stored as a *directory volume* or *Zip64 volume*. Both, digital traces and meta-data can be stored within this structure. A directory volume is a directory on the file system of a computer, which contains the segments of the volume named after a unique Uniform Resource Name (URN). A Zip64 volume contains a Central Directory at the end of the archive, which consists of a list of pointers to each digital trace within the volume. The format natively supports digital signatures to fulfil the security aspects *integrity* and *authenticity*. The *confidentiality* of the stored data can be preserved using an integrated stream based encryption scheme, which supports different access levels. Furthermore, AFF4 is designed to support distributed evidence.

A very similar data format, especially for the digital dactyloscopy, is introduced by Kiertscher et al. in [5]. It has a directory and a zip-file operation mode, too. In contrast to AFF4 it contains a tree of editions that can form a simple chain-of-custody to comprehend or audit the investigation process. It includes a hierarchical hash tree based on digital signatures to ensure *integrity* and *authenticity* for the data within the container. The underlying model supports encryption for the digitised traces and a portion of the meta-data. However, all encrypted data must be decrypted prior to any transformation of the container.

The database-centric approach of the *Fingerprint Verification Database (FiVe DB)* [6] has several advantages and disadvantages compared to the file based data exchange formats. It uses a watermarking approach for the digitised traces. The compression and difference expansion based watermark is embedded within the areas of the data, which contain the fingerprint. Those areas are compressed to gain storage for the meta-data. The embedded data is divided into a public and a private (encrypted) part. The latter contains the original fingerprint impression to ensure privacy. The embedded data contains digital signatures to ensure authenticity and integrity. The required location map for embedding areas is embedded throughout all data using a difference expansion approach. The hybrid database approach [6] employs user-defined functions to insert and read digitised traces. Those functions verify the authenticity and integrity of the transferred and stored data. Furthermore, it is easily possible to log any access to the data to create a chain-of-custody. However, *FiVe DB* requires a direct connection to the database to transfer the data. Alternatively, the watermark protected digitised traces can be exchanged as files, which enables a verification of the *authenticity* and *integrity* and ensures the *confidentiality* by the encryption of the private data. However, without the database the chain-of-custody information are quite limited within the watermark, due to the limited embedding capacity.

V. TECHNICAL DESIGN PROPOSAL

In this paper we focus on the challenges of the digitisation of the investigation of fingerprint traces. Our technical design proposal is derived from the process model for the digital dactyloscopy ([4], see Section IV.A). In contrast to the process model we primarily regard the transfer of digitised fingerprint traces (Figure 1).

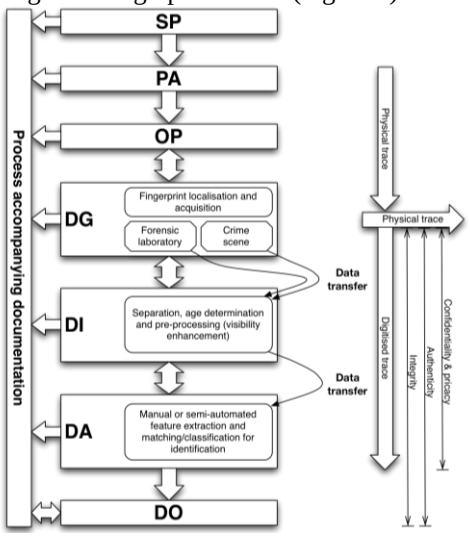

Figure 1. Our technical design proposal for a fingerprint scanning and analysis system.

The technical design has to cover two possible use-cases: *on crime scene trace acquisition* and the *acquisition in a forensic lab*. Since we focus on the newly digitised part of the forensic investigation, mostly the phases of *data gathering (DG)*, *data investigation (DI)* and *data analysis (DA)* are relevant including the data transfer between the phases. The technical design of a fingerprint scanning system must address the security aspects of *integrity* and *authenticity* for the gathered and processed data to be able to detect any modification (see Section IV.B). Thus, the final documentation should contain enough data to verify the integrity and authenticity of the data throughout the investigation process. Furthermore, it might be necessary to address the confidentiality of the acquired data to preserve privacy (see

Section III). This is especially needed if the digital traces are transferred. A criminal court proven design requires a detailed chain-of-custody for both, the digitised trace and the physical object containing the trace (see Section II.C.1).

With the data gathering (DG) the digitised trace is acquired. It is very important to retain a link between the physical object and its digital pendant or pendants. Therefore, multiple additional information, or meta-data, must be recorded. Such data includes various information, e.g., who acquires the trace, where is the trace acquired (especially for an on crime scene acquisition), when is it acquired, how are the environmental conditions during the acquisition or for which case are the traces acquired.

Afterwards, the collected data is transferred for a detailed investigation. This might include the transfer over insecure channels, e.g., if the data is send directly from a crime scene to a forensic investigation agency. It is crucial, that no data is altered or leaked during the transfer to preserve the evidentiary value and the confidentiality also as a pre-requisite for privacy. In the following *data investigation* the traces are prepared for the manual analysis.

During the *data investigation (DI)* the age of a fingerprint might be determined, overlapping fingerprints might be separated and the visual image of the ridge pattern might be enhanced for a better visibility of features during the analysis. However, at least the separation and the visibility enhancement involve an alteration of the original data. Thus, all parameters how the data is altered must be recorded and the original data must be accessible, too.

After the data investigation, the data are transferred to dactyloscopic experts for the extraction of biometric features and the subsequent identification of the fingerprint trace. In this *data analysis (DA)* phase additional data transfers might be necessary: transfer of the data to other forensic investigation agencies for the verification of the results (see ACE-V methodology [1]) or the transfer of the data for the comparison with AFIS databases (see [1]). The authenticity, integrity and confidentiality of the transferred data and the whole transfer process must be ensured because it might include insecure communication channels.

If a particular trace is identified a final documentation is created. Similar to the ACE-V methodology [1], this concluding result of the investigation should contain all investigation results. The digitised trace itself should not be included in the report. Thus, it is not required to ensure the confidentiality of the data because it does not contain any biometric traits. The integrity and authenticity of the documentation must be ensured in a digital representation.

Furthermore, the entire process needs to be documented within the process accompanying documentation.

In the following section, we exemplarily evaluate data formats according to their suitability for a future fingerprint scanning and analysis system. For that we derive the following technical requirements from our design proposal:

1. Authenticity protection,
2. Integrity protection,
3. Confidentiality/privacy protection,
4. Ability to store multiple traces and intermediate results of the investigation,
5. Ability to store various meta-data.

The requirement of a chain-of-custody can be fulfilled if the format supports all of the technical requirements except the confidentiality protection. The process accompanying documentation, e.g., from secure logging facilities, should be stored as meta-data within the file format.

VI. ANALYSIS OF FORENSIC DATA FORMATS

In this section, we analyse data formats towards their suitability for a future latent fingerprint scanning system. The *data format for the interchange of fingerprint, facial & SMT information* (ANSI/NIST-ITL 1-2000) [18] is already used in forensic investigations for the data exchange between different AFIS databases. Hence, it could be seen as generally accepted and should fulfil the legal requirements (Section III.A). However, this format does not support any techniques to preserve the privacy or confidentiality of the transferred data. Moreover, it does not preserve the integrity or the authenticity of the transferred data. Only a digital image of the signature of the acquisition officer is included within the file. The format supports multiple samples of different biometric traits and user-defined meta-data. Thus, at least the technical requirements 4 and 5 from our technical design proposal in Section V are addressed.

The *Advanced Forensics Format (AFF4)* [7] is not designed for the forensic analysis of biometric traits. However, it has several advantageous features for digitised forensics. The security aspects integrity, authenticity and confidentiality are sufficiently addressed by the data format if activated by the user or the used software. Furthermore, multiple traces or intermediate results and meta-data can be stored in this file format, fulfilling our technical requirements for a future fingerprint scanning system. Moreover, the ability to access data remotely through encrypted streams and the embedded access restriction enables a distributed investigation while preserving the confidentiality as a prerequisite for privacy. Additionally, different traces on the same object can be stored within a single trace file as a digital representation of the physical evidence bag.

The container for the digital dactyloscopy [5] ensures the integrity, authenticity and, optionally, confidentiality of the stored data, too. It enables the storage of multiple traces and intermediate results within the container file. Additionally, meta-data can be stored within separate files in the container. Thus, the container format fulfils our technical requirements for a future fingerprint scanning system, too. However, if the concurrent access to different traces within the container is necessary it is required to clone the container, which requires a merging-strategy if the two containers are joined again.

The database-centric approach *FiVe DB* [6] significantly differs from the file based approaches. The processed image files fulfil our technical requirements *integrity, authenticity* and *confidentiality* by the embedded watermark. A limited amount of meta-data can be stored directly within the image file. However, it is not possible to store multiple traces or intermediate results within a single image. The advantage of this approach is the superior access restriction and automated logging facilities of the database management system. The

 ISBN: 978-1-61208-182-3

disadvantage is the limited support for a data exchange without direct access to the database.

Table 1 summarises our evaluation for the data formats.

TABLE I. SUMMARY OF OUR EVALUATION RESULTS FOR THE STORAGE AND TRANSFER OF DIGITISED TRACES (+ REQUIREMENT FULFILLED; - REQUIREMENT NOT FULFILLED)

Technical requirement Storage / transfer	ANSI/NIST-ITL 1-2000	Advanced Forensics Format (AFF4)	Container for the digital dactyloscopy	FiVe DB
Authenticity protection	-/-	+/+	+/+	+/+
Integrity protection	-/-	+/+	+/+	+/+
Confidentiality protection	-/-	+/+	+/+	+/+
Multiple traces / intermediate results	+/+	+/+	+/+	+/-
Meta-data	+/+	+/+	+/+	+/+

In conclusion, the current ANSI/NIST-ITL 1-2000 is insufficient for a future fingerprint scanning system due to the lack of any addressed security aspects. In general, the other formats in this exemplary evaluation are appropriate.

VII. CONCLUSION AND FUTURE WORK

In this paper we proposed a criminal court proved design for a new fingerprint scanning system. For that, we analysed current legal requirements and derived a new legal approach. We use this framework to introduce a potential design for a digitised latent fingerprint acquisition and analysis system. It aims at enhancing privacy and preserving anonymity. We preliminarily modelled the data flow and data transfer.

Subsequently, we derived technical requirements for data formats using the technical design proposal and the legal approach. Our exemplary analysis of data formats using our requirements indicates that the currently used ANSI/NIST-ITL 1-2000 format is insufficient especially regarding the security aspects integrity, authenticity and confidentiality and thus unsuitable for privacy preserving transfers over insecure communication channels. The other data formats are appropriate for a future fingerprint scanning system.

In future work different sensors and processing techniques should be evaluated towards their applicability in a fingerprint scanning system. Furthermore, the necessary amount of meta-data for the chain-of-custody should be analysed to fulfil the requirements of criminal courts. This might improve the evidentiary value of each trace, too.

ACKNOWLEDGMENT

The work in this paper has been funded in part by the German Federal Ministry of Education and Science (BMBF) through the Research Programme under Contract No. FKZ: 13N10820 and FKZ: 13N10818.

REFERENCES

[1] Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST), "The Fingerprint Sourcebook," NCJ 225320, 2011.

[2] S. A. Cole, "More than Zero: Accounting for Error in Latent Fingerprint Identification," Journal of Criminal Law and Criminology, Vol. 95, No. 3, pp. 985-1078, 2005.

[3] M. Hildebrandt, J. Dittmann, M. Pocs, M. Ulrich, R. Merkel, and T. Fries, "Privacy Preserving Challenges: New Design Aspects for Latent Fingerprint Detection Systems with Contact-Less Sensors for Future Preventive Applications in Airport Luggage Handling," in: Biometrics and ID Management, LNCS 6583, pp. 286-298, 2011.

[4] M. Hildebrandt, S. Kiltz, I. Grossmann, and C. Vielhauer, "Convergence of Digital and Traditional Forensic Disciplines: A First Exemplary Study for Digital Dactyloscopy," in Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security (MM&Sec '11), pp. 1-8, 2011.

[5] T. Kiertscher, C. Vielhauer, and M. Leich, "Automated Forensic Fingerprint Analysis: A Novel Generic Process Model and Container Format," in: Biometrics and ID Management, LNCS 6583, pp. 262-273, 2011.

[6] M. Schäler, S. Schulze, R. Merkel, G. Saake, and J. Dittmann, "Reliable Provenance Information for Multimedia Data Using Invertible Fragile Watermarks," In 28th British National Conference on Databases (BNCOD), LNCS 7051, pp. 3-17, 2011.

[7] M. Cohen, B. Schatz, and S. Garfinkel, "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow," in Digital Investigation, 6(Supplement), pp. 57-68, 2009.

[8] BVerfGE (Bundesverfassungsgerichtsentscheidungen, respectively, collection of decisions of the Federal Constitutional Court of Germany) 110, 1 (22 f.), 1996; 82, 106 (118 ff.); 74, 358 (369 ff.); 35, 311 (320); 19, 342 (347 f.).

[9] B. Kasper, "Freie Beweiswürdigung und moderne Kriminaltechnik," Hamburg 1975, p. 119.

[10] For data security BVerfGE 125, 260 (para. 224), 2010; also § 17 para. 1 subpara. 2 Data Protection Directive 95/46/EC.

[11] A constitutional safeguard according to BVerfGE 125, 260 (224).

[12] In detail A. Roßnagel and P. Schmücker, "Beweiskräftige elektronische Archivierung - Bieten elektronische Signaturen Rechtssicherheit?," Bonn2006, pp. 13 ff.

[13] M. Knopp, "Digitalfotos als Beweismittel," in Zeitschrift für Rechtspolitik, 2008, 156 w. f. r.

[14] S. Tietze and K. Witthuhn, "Papillarleistenstruktur der menschlichen Handinnenfläche (Band 9)," Luchterhand, 2001, p. 76.

[15] Bundesgerichtshof, decision of 25.09.2007 – (4 StR 348/07).

[16] Pfitzmann, A., Informatik-Spektrum 10/2006, p. 353.

[17] S. Kiltz, M. Leich, J. Dittmann, C. Vielhauer, and M. Ulrich, "Revised benchmarking of contact-less fingerprint scanners for forensic fingerprint detection: challenges and results for chromatic white light scanners (CWL)", Proc. SPIE 7881, 78810G, 2011.

[18] The INTERPOL AFIS Expert Group, "Data format for the Interchange of Fingerprint, Facial & SMT information", INTERPOL Implementation Version 5.03 (ANSI/NIST-ITL 1-2000), [Online]. Available: https://www.interpol.int/Public/Forensic/fingerprints/RefDoc/ImplementationV5.pdf, 2011 [last checked 19.11.2011]

[19] National Institute of Standards and Technology, "CBEFF Common Biometric Exchange Formats Framework", NISTIR 6529-A, [Online]. Available: http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf, 2004 [last checked 19.11.2011]

[20] A. Pfitzmann, and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", v0.34, [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, 2010 [last checked 22.11.2011]

[21] S. Kiltz, A. Lang, and J. Dittmann, „Taxonomy for Computer Security Incidents", Cyber Warfare and Cyber Terrorism, pp. 412-417, ISBN 978-1-59140-991-5, 2007.