FROM BIOMETRIC TO FORENSIC HASHING: CHALLENGES IN DIGITAL CRIME SCENE TRACE ANALYSIS

Claus Vielhauer[1,2] , *Jana Dittmann*[1,3]

[1]Research Group Multimedia & Security, Otto-von-Guericke-University of Magdeburg, Germany
[2]Brandenburg University of Applied Sciences
[3]The University of Buckingham, Buckingham, United Kingdom
claus.vielhauer@fh-brandenburg.de, jana.dittmann@iti.cs.uni-magdeburg.de

ABSTRACT

The known *BioHash* concept introduced e.g. for handwriting biometrics offers possibility of template protection or to derive individual keys (e.g. crypto keys for further protection). In our paper we introduce two forensic use cases: (A) the forensic investigation of a *BioHash* found during digital forensics and (B) the application of the *BioHash* to latent crime scene traces in digitized forensics. Firstly, we elaborate the design of the *BioHash* in the known two operation modes with their essential parameter settings. Secondly we analyze, which forensic information can be derived and interpreted from publicly available data by introducing four investigation purposes. Further, we show that the *BioHash* can be used for a privacy-preserving search or to enhance reproducibility of varying features in crime scene forensics.

Index Terms— Biometrics, Passive forensic analysis

1. INTRODUCTION

In the field of biometric user authentication, biometric hashing has recently shown its potential as one possible approach towards template protection to ensure confidentiality and privacy issues of biometric data. In this context, *Biometric Hashing* refers to the transformation function onto the protection domain and the so-called *BioHash* data representation). Several approaches are described in the literature, considering security as well as reproducibility aspects, often being conflicting properties that need to be balanced. In this work we discuss and introduce potential application scenarios of biometric hashing in digital forensics and in crime scene trace analysis. The work is motivated based on the work in the EU COST action IC1106 Integrating Biometrics and Forensics for the Digital Age (http://ic1106.uniss.it/, 2015) or from [7]. In particular we suggest and study **two novel application cases**:

A) *BioHash* as digital forensic evidence with its possibility of forensically analyze the hash as piece of evidence, e.g. questioning what do we see and can derive from the found *BioHash* itself (forensic investigation of the *BioHash* value found). Here we are motivated from Soft Biometrics providing for a biometric modality some general findings such as identification of left or right handwriting or device properties from the biometric sensor.

B) *Biometric Hashing* applied to crime forensic traces found and captured at the physical crime scene in the field of digitized forensics as privacy preserving forensics approach with its ability to perform privacy preserving identification, verification, individualization and the possibility to search for individual or group properties (as proposed in case A - derived from Soft Biometrics).

For case A, we exemplarily select and elaborate handwriting modality data found as *BioHash* in a reference storage or in any memory storage by means from IT forensics as digital evidence on a computer system. **For case B**, we introduce general application purposes (e.g. also applied to fingerprint marks) and show additionally individualization tasks on the example of fiber traces for digitized latent crime scene traces. **For both cases**, we adopt from the insights of the known *BioHash* from handwriting [1] and suggest appropriate parameter settings for the novel application of biometric hashes in forensics. The concept is based on the idea of a parameter based generation of helper data (denoted as interval matrix) during enrollment and subsequent feature-wise transformation (interval mapping) during the hash generation process. This approach has been extensively studied with respect to parameter optimizations during enrolment, as well as its security properties related to non-reversibility and key space. Our goals are to identify and summarize **important design criteria** such as **operation modes** of the *Biometric Hashing* either *Hash Generation Mode* (i.e. robust intra-class reproducible *BioHash* generation, with inter-class bit sensitivity property) or *Verification Mode* (hashing used by allowing a distance based on a threshold for achieving stability without non-bit sensitivity), and algorithmic requirements. Additionally, we compare the design pattern in biometric and forensic domain to give important **guidelines for implementation and configuration**.

The paper is structured as follows: We first summarize the application areas of the *BioHash* from [1] as introduced for handwriting in the biometrics domain with two general operation modes and its essential parameters. Secondly we introduce our two use cases A and B by identifying the possible relevant forensic questions and goals (on the example of handwriting and fiber traces) as well as the potential relevant operation modes with its parameter settings (by considering beside a distance measure also an automated classification). Thirdly we summarize our

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

major findings and identify future work issues on the example of latent fingerprint for the community.

2. BIOMETRIC HASHING IN BIOMETRICS

As introduced in [1], *Biometric Hashing* in the biometric domain has the overall goal to ensure privacy-preserving template protection or to use the hash to derive and generate individual keys from it. As shown in Fig. 1, on the example of dynamic handwriting biometrics, the human handwritten input is acquired with a biometric sensor (such as digitizer tablet, writing pen or even today with fingers on a touch screen). The input signals undergo a pre-processing, mainly to remove temporal outliers in the writing process and to normalize the spatial writing area. From the pre-processed signals, feature vectors are calculated, where each feature component represents one statistical integer value derived from the entire input signal. Thus, the total number of statistical features calculated (i.e. 69 in the original publication [1]) determines the dimensionality of the resulting feature vector (and thus the dimensionality of the resulting *BioHash*). Actual *BioHash* vectors *bh* are then calculated by an interval mapping operation, supported by **helper data**, including so-called ***Interval Matrix, IM*** and others, as described in the coming subsection.

2.1. Helper Data

The Interval Matrix *IM* is being generated individually for each user of the biometric hashing system during an penrollment process (as common in biometrics) and is conceptionally based on the idea of statistically analyzing the intra-class variation of each feature component and each subject separately. As a result, the *IM* contains feature-wise mapping intervals, which are used for re-quantization during the interval index mapping. The resulting interval indices represent the *BioHash* vector component values and are expected to ensure robust reconstruction. Details on the *IM* enrollment process are given in [1].

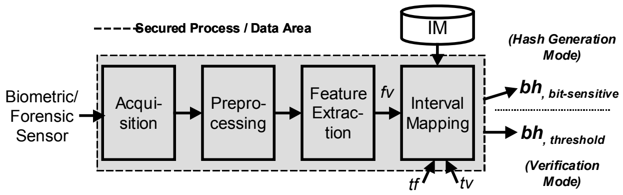

Fig. 1 *BioHash* pipline in Biometrics and Forensics.

Besides *IM*, **two parameters** are part of the helper data and influence the result of mapping an actual feature vector in *BioHash* domain: **tolerance factor (*tf*)** and **tolerance vector (*tv*)**:

The first has been introduced to parameterize the robust reconstruction of *BioHashes* in presence of intra-class variations greater than considered by the initial *IM* model during enrollment, with no consideration of inter-class properties. The *tf* simply linearly extends the lengths of mapping intervals for each of the features from *IM*, prior to matching by a constant factor, increasing the probability that any future actual feature value robustly maps to the same index, even if values exceed the ranges observed during enrollment. The *tf* is designed as an interval extension factor, a value of 0.5, for instance, means that the margins of quantization interval are expanded left and right by half of the initial interval length; the interval thus effectively doubles in length.

The second parameter, *tv*, follows the same intuition, however taking into account a prior empiric analysis of inter-class variability in feature space for each individual feature vector component. Conceptionally, this approach follows the idea to avoid collision between features of any two different subjects by limiting interval expansion (as compared to *tf*), wherever inter-class variability is limited. Consequently *tv* is represented by a vector of interval expansion factors, having the same dimensionality as *bh*.

As can be seen, both parameters *tf* and *tv* are crucial in the process to ensure robust reconstruction of *BioHashes* on the intra-class scope, with increasing values leading to higher probabilities for reconstruction of identical *BioHash* vectors for each individual subject. However, this goes along with a trend of increasing probably of different subjects generating identical *bh*, a situation which is referred to as *collision*.

2.2. Hash Generation versus Verification Mode

As already introduced in the first section, two general operation modes exist: *Hash Generation Mode* (i.e. optimize towards intra-class reproducibility with the property of bit sensitivity w.r.t. different non-identical subjects) or *Verification Mode* (hashing used as template representation by allowing a threshold–based comparison in *BioHash* domain, with no claim on bit sensitivity).

Obviously, *BioHash* values in *Hash Generation Mode* (referred to as $bh,_{\ bit\text{-}sensitive}$ in Fig. 1) are adequate for subsequent cryptographic calculations, for example cryptographic hashing, if the actual reproduction rate is sufficiently high and the collision probability remains at an acceptable level. Of course, as for all biometric concepts, both aspects cannot be guaranteed and in fact errors in both classes (reproduction/collision) are expected and need to be evaluated empirically. For this purpose the error rates Reproduction Rate (*RR*), Collision Rate (*CR*) and the combined Collision Reproduction Rate (*CRR*) have been introduced in [2]. These error rates are determined by calculating the *Hamming Distance* $HD(bh_1, bh_2)$ (i.e. the number of non-identical components) between two given *BioHash* vectors bh_1, bh_2 as follows: the sum of occurrences of $HD(bh_1, bh_2)=0$ for any bh_1, bh_2 belonging to different non-identical subjects during inter-class testing is related to the total number of inter-class tests, thus representing the observer collision ratio (i.e. *CR*). Respectively, the sum of occurrences of $HD(bh_1, bh_2)=0$ for any bh_1, bh_2 belonging to the same identity, related to the total number of all *intra-class* tests, determines the ratio of successful reproductions, i.e. the *RR*. In other words, *CR* represents the observed ratio of identical inter-class *BioHashes* and *RR* the inter-class ratio of successful reconstruction of identical *BioHashes*. With *CR* and *RR* denoting an empirically observed probability of inter-class collisions and successful intra-class reconstructions of *BioHashes* respectively, CRR is defined as the average of *CR* and not-reproducibility rate (i.e. *1-RR*), as per Equation 1.

$$CRR = \frac{CR + (1 - RR)}{2} \tag{1}$$

Since *BioHash* values determined in *Verification mode* (*bh, $_{threshold}$* in Fig. 1) are used for threshold-based verification based on distance functions such as Hamming, Euclidean or Canberra distances[3], in these scenarios, the common biometric error rates (i.e. False Rejection Rate *FRR* for the percentage of falsely rejected authentic users and *FAR* for false acceptances in verification mode and/or Identification Rate *IR* in identification mode) can be determined to express empiric error characteristic.

Essential parameter settings: in [2], the impact of *tf* and *tv* has been thoroughly evaluated based on a test data set for dynamic handwriting. It consists of data from 39 test subjects, 10 samples of 5 different semantics (public PIN "77993", secret PIN, pseudonym, symbol and a hand written answer to the question "Where are you from?"), collected by a Toshiba® M200 Portegé tablet PC. The data set is split into 3 parts, the first of which is used for enrollment (i.e. *IM* generation), the second for *tf* tuning and feature selection and the third set for actual evaluation in Hash Generation and Verification mode, while *tv* has not been set be empirical values (i.e. all *tv* components set to value 1). Regarding the feature set, [2] further uses an extension from 69 features (as in [1]) to 131 components and studies the performance of biometric error rates *RR/CR/CRR* and *FRR/FAR* in *Hash Generation* and *Verification Modes* respectively for the third part of the data set. In *Verification Mode*, a Hamming-Distance based thresholding has been applied for classification.

These experiments have been conducted with and without feature selection (to an intuitive target dimensionality of 60) by filtering and wrapping, using nine different methods. From the experiments, the following insights can be concluded w.r.t. the scope of this paper:

- In *Hash Generation Mode*, for all semantic classes, a local minimum regarding the *CRR* has been observed for a *tf* value in the interval *[2.0 .. 4.0]*. The lowest *CRR* (thus the best average accuracy w.r.t both error classes) value observed was *6,32%* for semantics "symbol" for *tf = 3.7.*
- In *Verification Mode*, the lowest *EER (5.27%)* was again observed for semantics "symbol" for *tf=1.5*. Further, the analysis of *EER* as function of *tf* indicate almost constant values for *tf* in the range of *[0 .. 1.5]* with no significant local minima. For values *[1.5 .. 10.0]*, increases in *EER* can be observed for all semantics.
- For both *Hash Generation* and *Verification Modes*, from the studied feature selection methods, two strategies have shown best performance for the two feature selection concepts filter and wrapper: anova/anova-2class for the classes of (computationally simple) filter methods and best-first for (computationally more complex) wrapper-based feature selection methods.

From these insights, the following essential parameters can be summarized with regards to the different modes of *Biometric Hashing* (Table 1, Note, IM being an individual enrolled data, not included here).

In order to ensure privacy (confidentiality of the original biometric signals captured), from the security perspective, the following parts need to be considered regarding data and parameters:

a) can be *kept public*: *IM* of each subject (as reverse projection of *bh* by means of *IM* onto original signal data seems to be infeasible to date [4]). Further, *tf* and *tv* can also be considered public parameters.

b) need to be *stored in a secure manner*: Obviously all data and process steps prior to the generated *IM* and *bh* in the process model (see in the area surrounded by dashed lines in Fig. 1) need to be secured, as well as the system integrity and authenticity of the complementary *Hash Generation* and *Verification* process, to avoid result manipulation by attackers.

For the later aspects, systems needs to be designed to enable a temporary secure storage and processing e.g. supported by cryptographic means, and/or physical protection schemes such as smart cards systems. Further, to avoid forensic recovery, the memory used for storage and calculation based on secure data should be overwritten by pseudo-random values after their deallocation in memory.

Bio Hashing Mode	tf	tv	Feature Selection (Filter)	Feature Selection (Wrapper)
Hash Generation	2.0 – 4.0	(1,…,1)	Best-First	Anova/ Anova 2class
Verification	0 – 1.5	(1,…,1)	Best-First	Anova/ Anova 2class

Table 1. Both *BioHash* modes with their essential parameter settings (derived from observed scenarios in [2]).

3. FORENSIC USE CASES

In the following we discuss our two identified use cases A and B in the forensic domain.

3.1. *BioHash* value for interpretation as digital forensic evidence (use case A)

Use case A is motivated by a situation, where during a forensic investigation a *BioHash* vector $bh,_{investigate}$ is found by IT forensic means on the target system. Besides $bh,_{investigate}$, here we assume that we find at least the public available data as summarized in section 2: the *IM, tf* and *tv* related to $bh,_{investigate}$ (i.e. the public transformation parameters that actually led to the found vector). Additionally, secured data, as discussed above and outlined in the dashed area in Fig. 1 could be available from the forensic recovery (for example because it has not been protected on system level). While this later information of course leaks personal data about the originator trivially (e.g. by access to the biometric raw measurement), in our paper we do not discuss this case further and focus the case of availability of public data only. We now analyze which forensic information can be derived and interpreted from this publicly available data by considering four investigation purposes. Firstly, independently of the mode (*Hash Generation or Verification*), information on ***i) Soft Biometrics*** & ***ii) Sensometrics*** can be achieved by estimation of the original feature space based on the public data: ***i) Soft Biometrics*** generally describes biometric analysis that allow group assignments of individuals rather than individualizations, which today are common particularly (but not limited to) in surveillance applications. Examples from the variety in soft biometric traits are estimations of body height, or age/gender/hair color by video analysis. In a generalized view, any soft biometric feature can be regarded as one statistical term of a complete biometric measurement (e.g. the calculation from the estimated body height from a video recording or the estimation of the size of a signature). To this end, the concept of Soft Biometric features can be adopted to any biometric modality and any possible estimation of meaningful feature values from $bh,_{investigate}$ and the public data can reveal relevant forensic information. For example, as part of the original feature set as suggested for biometric hashes for handwriting in [1], statistical values for fundamental information about the writing trace are included, such as total write time, total number of pixels, average velocity in *x* and *y* direction. Within their work on reverse-engineering methods on biometric hashes, Kümmel et al. have shown that every biometric hash actually leaks information about the value range of its originating feature vector, provided the helper data is available [4]. Since due to the interval mapping concept inherent to the biometric hashing process, no inverse function exits, they propose a reverse mapping of biometric hash vector component $bh_{investigate,i}$ onto the middle of the original mapping interval according to the following Equation 2:

$$fv_{estimate,i} = bh_{investigate,i} * \Delta I_i + \Omega_i + \frac{\Delta I_i}{2} \qquad (2)$$

Here, *i* stands for the component index of each single value within the vectors (e.g. $i \in [1 .. 69]$) for the feature ses from [1]). $b_{investigate,i}$ denotes the *BioHash* vector component to be reverse mapped and Interval Length Vector ΔI and an Interval Offset Vector Ω are the two vectors that form the interval matrix: $IM= (\Delta I, \Omega)$. The resulting estimation for the original feature value is given by each of the components of vector $fv_{estimate}$ after the reverse mapping. Further, the actual true bounds of the true original feature vector components $fv_{original,i}$ can per derived from Equation 3.

$$bh_{investigate,i} * \Delta I_i + \Omega_i \leq fv_{original,i} \leq (bh_{investigate,i} + 1) * \Delta I_i + \Omega_i \qquad (3)$$

While the focus of [4] was to illustrate how ultimately artificial original biometric signals can be constructed from these reverse mapped features, quite obviously concepts is valuable for soft biometrics, if the meaning of the individual features are known. For the particular example of handwriting as described in [1], this includes forensically relevant information such as approximate writing duration, size of the handwritten sample and area density of the writing on the surface, which can be bounded and estimated and are thus of forensic relevance. ***ii)*** A definition of ***Sensometrics*** in the domain of biometrics and forensics has been defined by Oermann et al. in [5]: *"(...) sensometrics as the application of methods for the analysis and determination of a particular sensor (device) an original digital sample is sampled with, whereby the actual context in which the original sampling has been performed can vary. For example, for identifying digital cameras, any photographic image can be taken into account, whereas for identifying pen digitizer, sensors for capturing handwriting samples such as signatures can be analyzed.(...)"*. In the same publication, authors describe a method to identify pen digitizer sensors from a set of 23 in total (some of which are identical hardware but used in different configuration), which have been used to collect a total of app. 20.000 biometric handwriting samples. Based on a feature set composed of 5 values (altitude type, pressure level type, pressure difference value, time difference value, and average sampling rate) and using a decision tree model, they experimentally show that 12 out of the 23 devices could be identified with 100% accuracy. Also, another six showed correct identification rates of over 90%. However, authors report two major restrictions of their concept: differentiation of pen digitizers with the same sensor technology could not be achieved and low resolution devices tend towards higher false identification rates.

Adopting this idea for the forensic analysis of *BioHashes* and under the same assumptions as in our discussions on Soft Biometrics, the estimation of original feature values can reveal information about the sensor device, if the interpretation of their values is known. Again referring to the handwriting biometrics example and according to [5], features such as sampling rate, min. and max. pressure values (or the absence thereof), presence/absence of pen angle information and ranges of *x* and *y* positions can potentially achieve system identification in many cases. These terms are either part of the original feature set of the original *BioHash* concept [1] or can be derived from multiple original features. Thus, if estimation of the original feature becomes feasible, sensor identification can be performed even based on a found *BioHash* vector, the public data and knowledge about the feature extraction.

Secondly, ***iii) Key Estimation/ Key Search Space Reduction*** are additional possible forensic effects in use case A, provided that $bh,_{investigate}$ was generated in the *Hash Generation Mode.* Recall that here we expect a robust intra-class reproducible *BioHash*, with inter-class bit sensitivity property, as introduced in the previous section. The first forensic purpose of such finding applies, if the *BioHash* is involved in any subsequent cryptographic data processing within the target system. In this case, knowledge of $bh,_{investigate}$ provides side information for cryptoanalysis or even the complete credential themselves. To give an example for the first situation, if *BioHashes* are used as partial seed to any key generation (e.g. by using is as seed in conjunction with an additional password component), knowledge of the *BioHash* can significantly reduce the effective key search space and thus raise the potential for key recovery. Thirdly, ***iv) Forensic Identification*** can be achieved, if the *BioHash* was generated in *Verification Mode* (recall this refers to BioHashing without non-bit sensitivity by allowing a distance based analysis with a threshold) and in case no subsequent cryptographic transformations have been applied to $bh,_{investigate}$, the forensic value is given by the possibility to perform similarity analysis: assume the observer in possession of a collection of reference of known subjects, produced under similar conditions such as identical trait and sensor specifications, a simple similarity search can be performed. Based on minimum distance between $bh,_{investigate}$ and all reference samples, the identity of the originator can be obtained with high probability from the list of closest matches, given originator samples of $bh,_{investigate}$ are actually part of the reference set. However, if no references of the originator of $bh,_{investigate}$ are in the reference set, the search will still result in a match, thus leading to wrong identification.

3.2. Crime scene traces analyzed as *BioHash* (B)

In an digitized forensic investigation, where traces such as latent traces of fingerprint marks, handwritings or fibers are found at a crime scene and digitized for further analysis, the *Biometric Hashing* can help in performing **B.1) privacy preserving search** on all traces captured or **B.2) the reproducibility of varying features** can be used for achieving stability in noisy or partially available traces.

Privacy preserving forensic analysis B.1): for identification or verification as explained in section 2 and for individualization (one-to-one) or identification (one-to-many) search purposes for individual or group properties as proposed in section 3.1, the concept of *Biometric Hashing* can be adopted if: a feature set of constant size and order can be obtained after any adequate pre-processing in the process chain and a sufficient amount of test data (empirical basis) for appropriate parameters estimations (*tf* ad *tv*) are available.

From today's perspective, this concept seems quite feasible for forensic fingerprint analysis, since numerous features have been discussed in the literature, many of which appear appropriate for the process (e.g. ridge density thickness, minutiae statistics etc.). However, within the paper scope, this idea is proposed conceptionally, but to best of our knowledge, it has not been performed practically yet.

For **supporting reproducibility B2)**, the application of *Biometric Hashing* for fiber forensic traces based measurements by thin film reflectometery has been introduced in [6]. Here the forensic goal is to perform either *group identification* amongst five different fibric type classes (acrylic, polyester, alpaca, sheep wool, cotton) or *individualization* (of five color variations within each class). This is achieved by performing hyperspectral scans at a fixed number of measurement points on the fiber surface of each sample. For each measurement point, a 2048 dimensional feature vector is obtained, representing 16-bit quantised reflectance spectra values (energy) for a wavelength range between *844 - 163 nm* in steps of approx. *0.33 nm*. Authors experimentally evaluate four different setups for the lateral resolution, leading to 8, 14, 68 and 340 instances of 2048-dimensional feature vectors per sample. For each sample, half of the instances (4, 7, 34, 170) have been used for *IM* generation and the other half for *bh* calculations, with both *tf* and *tv* trivially set to *0* as *BioHash* is here used in *Verification Mode* only. Based on a test set size of 50 specimens and applying various classifiers of the Weka machine learning software (http://www.cs.waikato.ac.nz/ml/index.html, 8.2.2015) have been trained, on the original feature vectors as well as on the obtained *BioHash*es. Authors experimentally show the tendency that classification in *BioHash* domain may outperform raw feature spaces. Particularly the first classification tests in *individualization* showed improvements from appl. 94% for raw features to 100% by use of *BioHashes*. Improvements have also been observed in all cases of *identification* – throughout the four different scan resolutions, leading to the conclusion that *Biometric Hashing* should be further studied to improve reproducibility for forensic fiber analysis.

4. MAJOR FINDINGS AND SUMMARY OF FUTURE WORK

In our paper we have reviewed the known *BioHash* from handwriting to introduce and elaborate two forensic uses cases by discussing operation modes and parameter settings. Future work needs to look into appropriate feature spaces with its relevant parameters. For example main issues are for case A the investigation of further soft biometric and device depending features or for B the feature space design for partially versus full traces.

5. ACKNOWLDGEMENTS

This work has been funded in part by the German Federal Ministry of Education and Science (BMBF) through the Research Program under Contract No. FKZ: 13N10816 and FKZ: 13N10818. We thank the paper reviewers for their fruitful comments and the support from the EU COST action IC1106 Integrating Biometrics and Forensics for the Digital Age (http://ic1106.uniss.it/, 2015).

REFERENCES

[1] C. Vielhauer, *Biometric User Authentication for it Security - From Fundamentals to Handwriting*, Springer - Advances in Information Security 18, 2006

[2] A. Makrushin, T. Scheidat, C. Vielhauer, *Handwriting Biometrics: Feature Selection based Improvements in Authentication and Hash Generation Accuracy*, Proc. Biometrics and ID Management, Springer, 2011

[3] T. Scheidat, C. Vielhauer, J. Dittmann, *Handwriting verification – Comparison of a multi-algorithmic and a multi-semantic approach*, in *Image and Vision Computing*, vol. 27, Elsevier, 2009, pp. 269–278

[4] K. Kümmel, C. Vielhauer, *Reverse-engineer Methods on a Biometric Hash Algorithm for Dynamic Handwriting*, in Proc. ACM SIGMM Multimedia and Security Workshop, ACM, 2010, pp. 67-72

[5] A. Oermann, C. Vielhauer and J. Dittmann, *Sensometrics: Identifying Pen Digitizers by Statistical Multimedia Signal Processing,* in Proc. SPIE Electronic Imaging - Multimedia on Mobile Devices III, Vol. 6507, 2007, pp 65070I-1-65070I-12

[6] C. Arndt, J. Dittmann and C. Vielhauer, *Spectral Fiber Feature Space Evaluation for Crime Scene Forensics Traditional Feature Classification vs. BioHash Optimization*, in 10th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, 2015, Berlin, Germany, DOI:10.5220/0005270402930302

[7] Meuwly, D. and Veldhuis, R.N.J., *Forensic biometrics: From two communities to one discipline*, in: Proc. International Conference of the Biometrics Special Interest Group (BIOSIG) 2012, Darmstadt, Germany. pp. 1-12. ISSN 1617-5468 ISBN 978-1-4673-1010-9