Towards reproducible results in authentication based on physical non-cloneable functions: the forensic authentication microstructure optical set (FAMOS)

Sviatoslav Voloshynovskiy [#1], Maurits Diephuis [#2], Fokko Beekhof [#3] Oleksiy Koval [#4], Bruno Keel [*5]

[#] *University of Geneva, 7 route de Drize, CH 1227, Geneva, Switzerland*
[[#1] svolos, [#2] maurits.diephuis, [#3] Fokko.Beekhof, [#4] koval]@unige.ch

[*] *U-nica Systems, Industriestrasse 4, 7208, Malans, Switzerland*
[5] Bruno.Keel@u-nica.com

***Abstract*—Nowadays, the field of physical object security based on surface microstructures lacks common and shared data for the development, testing and fair benchmarking of new identification and authentication technologies. To our knowledge, most published results are based on proprietary data that also often lacks the necessary size for statistically significant results and conclusions. Therefore, in this paper, we introduce the first publicly available documented database for the investigation of physical object authentication based on non-cloneable surface microstructure images. We have built an automatic system suitable for massive acquisition of microstructure images from flat surfaces under different light conditions and with different cameras. The samples are acquired several times, and resulting images are aligned, labelled and online available to the public for further investigation and benchmarking of new methods. In this paper, we present the statistical properties for the images originating from 5000 unique carton packages acquired 6 times each with two different cameras. Furthermore, we derive statistical authentication frameworks for the original, the random projected and binarized domains presented together with all empirical results.**

I. Introduction

Identification and authentication of physical objects based on microstructure images represents one of the most attractive and challenging problems of physical world security. The cheap enrollment, the non-invasive character of the protection, the easy and fast verification by non-experts make this protection scheme highly competitive and attractive for large-scale mass market applications. The core of this protection is based on the uncloneable character of the surface microstructures and their uniqueness which make it similar to human biometrics. Therefore, the corresponding identification and authentication technologies have many elements in common with biometric systems. The key elements of these systems are the selection of robust or invariant features, dimensionality reduction and finally quantization resulting into a binary representation of the original image known as a *binary template* or a *content fingerprint*.

WIFS'2012, December, 2-5, 2012, Tenerife, Spain.
The contact author is Prof. Voloshynovskiy (svolos@unige.ch).
978-1-4244-9080-6/10/$26.00

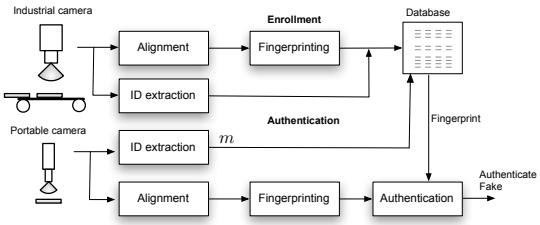
At the same time, digital content fingerprinting is an active field of research in multimedia applications requiring content identification, copy detection, tracking, filtering and authentication [1]. Many algorithms that are capable of withstanding various image processing and geometrical modifications for the digital media have emerged from this field [2]. In contrast, few results for physical object protection based on microstructures have been published [3]. Several reasons can be pointed out that explain the current situation. Primarily, it is the lack of publicly available databases containing a significant number of images of surfaces acquired using different cameras under various acquisition conditions. Secondly the field suffers from the proprietary character of the deployed technology which significantly restricts the involvement of the academic community. This problem is in part caused by the large-scale character of this particular application that requires massive acquisition, something that is difficult in a non-industrial environment. Finally, as a consequence of all the aforementioned factors, there is a lack of strict benchmarking rules both accepted in the academic community and in industry.

This paper will address the following open issues. It provides an online available forensic authentication microstructure image set comprised of 5000 unique samples, acquired 6 times with two cameras. It examines and models relevant statistical properties of the microstructure set. Feature extraction, dimension reduction and quantization are performed, analyzed and statistically modeled.

This paper is organized as follows: Section 2 contains the experimental setup and describes the acquisition process and resulting database. Real domain results are analyzed in Section 3 together with the statistical authentication framework for this domain. Random projection based domain conversion and dimension reduction is subject of Section 4, which also contains the empirical tests in this domain and the matching authentication framework. Similarly, in Section 5 results from the binary domain are presented. Sections 6 and 7 conclude the paper presenting conclusions and future work.

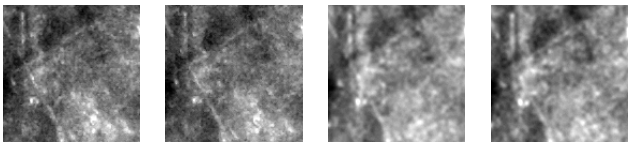
Notation: Scalar random variables are designated by capital letters X, and bold capitals $\mathbf{X}$ denote vector random variables. Corresponding small letters x and $\mathbf{x}$ denote their respective

(a)



(b)

Figure 1: The acquisition and authentication architectures, 1a shows the acquisition device, including the feeder, belt, camera, lighting and integrated computer screen, 1b the shows the enrollment and authentication framework.



(a) (b) (c) (d)

Figure 2: Multiple acquisitions of a single microstructure sample from Cam 1 (2a, 2b) and Cam 2 (2c, 2d). Histogram equalization was used for visualisation purposes.

realizations, where $\mathbf{x} = \{x[1], x[2], \ldots, x[N]\}$. The binarized version of $\mathbf{x}$ is represented by $\mathbf{b}_\mathbf{x}$. $X \sim p(x)$ indicates that the random variable follows $p_X(x)$. $\mathcal{B}$ indicates the Bernoulli distribution.

II. Experimental setup

To acquire a massive set of microstructure images under different conditions, an experimental industrial system was developed. Two color cameras, designated Cam1 and Cam2 respectively, are deployed above a conveyor belt that feeds the paper samples through the system. The system can process up to 20000 samples in a single run. Lighting is identical and consists of a white led ring light together with an angled one approximately 90mm above the surface. Cam1 has a resolution of 2592×1944 (5Mp) with a sensor size of 5.7×4.4mm and a pixel size of $2.2\mu m$. It has an optical magnification of $1 : 0.9$. Cam2 has a resolution of 1601×1201 (2Mp), a sensor size of 7×5.2mm, a pixel size of $4.4\mu m$ and no optical magnification. The entire setup is shown in Figure 1a.

To ensure accurate micro-structure extraction, samples are aligned using a printed mark. Cam1 images are down-sampled to match Cam2. Other than a conversion to grayscale, no preprocessing is applied, which ensures that future users are free to design their own preprocessing and feature extraction methods. The final micro-structure is a 128×128 pixel sized patch which is losslessly stored in a connected database. The FAMOS dataset contains 5000 unique samples, acquired with the two different cameras, three times each giving a total of 30000 images. Acquisition examples for both cameras of a single sample are shown in Figure 2.

The enrollment and authentication framework is shown in Figure 1b. In the enrollment stage, samples are acquired under industrial conditions using the fast camera Cam1. Following acquisition, the image is aligned using a printed mark after which a fingerprint is extracted from the micro-structure which is stored in a database together with the sample's identifier. Verification follows the same pipeline with the exception that it can be done somewhere externally with a handheld camera system that differs from the enrollment setup. After acquisition and alignment, the fingerprint is extracted and presented for authentication. The FAMOS database is published on `http://sip.unige.ch/famos`.

III. Direct domain

To establish a base-line for performance, the first tests are done in the real-domain. Furthermore, one can reasonably assume that working with the original high dimensional data should lead to the best performance. There are, however, a number of open issues. Primarily, the exact statistical models of the images and their distortions are unknown. A direct consequence of this is the fact that it is difficult to derive an optimal comparison metric. Shown in Figure 3 are the element-wise differences for different acquisitions from identical samples, for all cameras, in the direct domain together with a superimposed estimated Gaussian probability density function (pdf).

One can conclude that the Gaussian additive noise model can be used to approximately model the acquisition distortions under the assumption that the samples have been correctly synchronized using the printed mark. However, more accurate statistical models based on non-Gaussian pdf's might lead to a more accurate approximation.

To proceed with the statistical model of the observations one should develop an accurate model of $f(\mathbf{x}_i(m)|\mathbf{x}_j(m))$, where i and j denote the index of the acquisition from a sample with identifier m. This in itself is a challenging task and furthermore the model might be highly varying for different acquisition conditions and cameras. Consequently, it is often assumed that the acquisition distortions are additive and follow a Gaussian distribution with zero mean and variance σ_Z^2 which can be estimated from the experimental data.

Under these assumptions, one can consider the object authentication problem as the binary hypothesis test:

$$\begin{cases} H_0\text{: } \mathbf{y} = \mathbf{x}(n) + \mathbf{z}, \\ H_1\text{: } \mathbf{y} = \mathbf{x}(m) + \mathbf{z}, \end{cases} \tag{1}$$

where the hypothesis H_0 corresponds to the case when some object with the wrong identification number is presented to the system, and hypothesis H_1 denotes a valid case where the identification number is m. Following the assumption of the Gaussianity of the noise $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 \mathbf{I}_N)$, one can show that the sufficient statistic for the authentication problem, (1), formulated above, is the cross-correlation coefficient ρ_{xy} between vectors $\mathbf{x}$ and $\mathbf{y}$ [4].

Having chosen normalized ρ_{xy} as the measure of similarity, the *inter* and *intra* class were computed. The *intra*-class is built up from all ρ_{xy} values between acquisitions from identical labels. The *inter*-class is comprised of all ρ_{xy} values between acquisitions from non identical labels. The results for all camera combinations are shown in Figure 4, where 4a shows the normalized histograms of the *intra* and *inter* class.

It is important to note that ρ_{xy} for the *intra* class shows a small non-zero mean bias, which might be explained by the small correlation between microstructures, and closely follows a Gaussian shape. However, the *inter* class ρ_{xy} demonstrates non-Gaussian behaviour, similar to that observed in Figure 3.

To further characterize the performance of the object authentication system, the Receiver Operator Characteristic was determined. The corresponding ROC curves can be seen in 4b, and show the probability of miss (P_m) and of false-alarm (P_{fa}) which are derived using the Neyman Pearson lemma and the estimated probability density functions from 4a.

In the case where the cameras for enrollment and authentication are identical the best performance is observed. It is notable that the lower resolution Cam2 outperforms Cam1. As expected, the weakest performance is seen when the enrollment and authentication cameras are different. Contributing factors to this weaker performance are most likely the lighting, the resolution mismatch and the consequently needed downscaling prior to comparison.

IV. Random Projection based Fingerprinting

Motivated by earlier results [5], [6] we performed a domain conversion and dimension reduction to a domain where the microstructure and acquisition distortion statistics are quasi Gaussian.

Dimensionality reduction of the 128×128 micro-structure from image with identifier m, $\mathbf{x}(m)$, is done as follows:

$$\tilde{\mathbf{x}}(m) = \mathbf{W}^{L \times N} \mathbf{x}(m). \tag{2}$$

where $\mathbf{W}^{L \times N} \in \mathcal{R}^{L \times N}$. L is the length $\mathbf{W}^{L \times N}$ will map to, N is the length of the input column vector, which is 128^2. Random matrix $\mathbf{W}^{L \times N} = (\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_N)^T$ consists of a set of approximately orthonormal basis vectors, where all elements are generated as $W_i[j] \sim \mathcal{N}(0, \frac{1}{N})$, $1 \leq i \leq N, 1 \leq j \leq L$, and as such behaves as an approximate *orthoprojector* for which $\mathbf{W}\mathbf{W}^T \approx \mathbf{I}_L$ [1]. Deploying Gaussian basis vectors also guarantees that the projected vectors $\tilde{\mathbf{x}}(m)$ can be considered as realizations of a Gaussian source with a covariance matrix that converges to diagonal in probability [7]. It has been shown that random projections decorrelate data vectors amongst each other under certain assumptions.

The authentication problem can now be reformulated as hypothesis test with two hypotheses, H_1 models a fingerprint $\tilde{\mathbf{x}}(m)$ that is genuinely authentic, H_0 models a counterfeited or non-enrolled item $\tilde{\mathbf{x}}(n)$:

$$\begin{cases} H_0\text{: } \tilde{\mathbf{y}} = \tilde{\mathbf{x}}(n) + \tilde{\mathbf{z}}, \\ H_1\text{: } \tilde{\mathbf{y}} = \tilde{\mathbf{x}}(m) + \tilde{\mathbf{z}}, \end{cases} \tag{3}$$

where $\tilde{\mathbf{z}}$ is the Gaussian noise component.

Deploying the Neyman-Pearson decision rule, maximizing the probability of detection, the likelihood ratio test becomes:

$$\Lambda(\tilde{\mathbf{y}}) = \frac{p(\tilde{\mathbf{y}} \mid H_1)}{p(\tilde{\mathbf{y}} \mid H_0)} \gtrless \tilde{\eta}, \tag{4}$$

with the threshold $\tilde{\eta}$ chosen to satisfy the constraint $P_{fa} = \int_{\Lambda(\tilde{\mathbf{y}}) > \tilde{\eta})} p(\tilde{\mathbf{y}}|H_0) d\tilde{\mathbf{y}} = \alpha$ where $p(\tilde{\mathbf{y}}|.)$ is the distribution of $\tilde{\mathbf{y}}$ under the corresponding hypothesis and α is the desired constraint on P_{fa}. Assuming that the noise $\boldsymbol{Z}$ is Gaussian, $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 \mathbf{I}_L)$:

$$\begin{cases} H_0\text{: } \tilde{\boldsymbol{Y}} \sim \mathcal{N}(\tilde{\mathbf{x}}(n), \sigma_Z^2 \mathbf{I}_L), \\ H_1\text{: } \tilde{\boldsymbol{Y}} \sim \mathcal{N}(\tilde{\mathbf{x}}(m), \sigma_Z^2 \mathbf{I}_L). \end{cases} \tag{5}$$

Reformulating the decision rule (4) by taking the logarithm:

$$\log p(\tilde{\mathbf{y}}|H_1) - p(\tilde{\mathbf{y}}|H_0) \gtrless \log \tilde{\eta}. \tag{6}$$

Reducing the decision rule (6) to a sufficient statistic t:

$$t(\tilde{\mathbf{y}}) := \tilde{\mathbf{y}}^T (\tilde{\mathbf{x}}(m) - \tilde{\mathbf{x}}(n)) - \frac{1}{2}(\tilde{\epsilon}(m) - \tilde{\epsilon}(n)) \gtrless \tilde{\gamma}, \tag{7}$$

where $\tilde{\gamma} = \sigma_Z^2 \log \tilde{\eta}$ and $\tilde{\epsilon}(m) = \tilde{\mathbf{x}}^T(m)\tilde{\mathbf{x}}(m) = ||\tilde{\mathbf{x}}(m)||^2$ is the energy of the signal $\tilde{\mathbf{x}}(m)$ and $\tilde{\epsilon}(n) = \tilde{\mathbf{x}}^T(n)\tilde{\mathbf{x}}(n) = ||\tilde{\mathbf{x}}(n)||^2$ of signal $\tilde{\mathbf{x}}(n)$, characterized by:

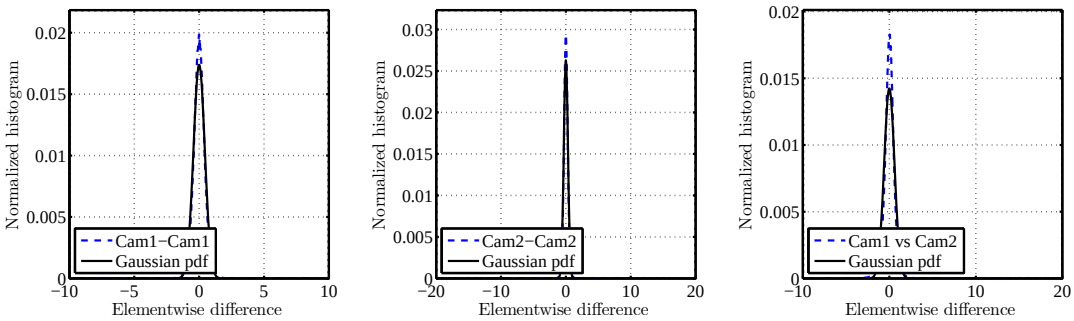
$$\begin{cases} H_0\text{: } T \sim \mathcal{N}(-\frac{1}{2}\tilde{d}^2, \sigma_Z^2 \tilde{d}^2), \\ H_1\text{: } T \sim \mathcal{N}(+\frac{1}{2}\tilde{d}^2, \sigma_Z^2 \tilde{d}^2), \end{cases} \tag{8}$$

where $\tilde{d}^2 = ||\tilde{\mathbf{x}}(m) - \tilde{\mathbf{x}}(n)||^2$. The probability of false alarm P_{fa} and miss P_m can then be formulated as:

$$\begin{cases} P_{fa} = Pr[T > \tilde{\gamma} \mid H_0] = & Q\Big(\frac{\tilde{\gamma} + \frac{1}{2}\tilde{d}^2}{\sqrt{\sigma_Z^2 \tilde{d}^2}}\Big), \\ P_m = 1 - Pr[T > \tilde{\gamma} \mid H_1] = 1 - & Q\Big(\frac{\tilde{\gamma} - \frac{1}{2}\tilde{d}^2}{\sqrt{\sigma_Z^2 \tilde{d}^2}}\Big). \end{cases} \tag{9}$$

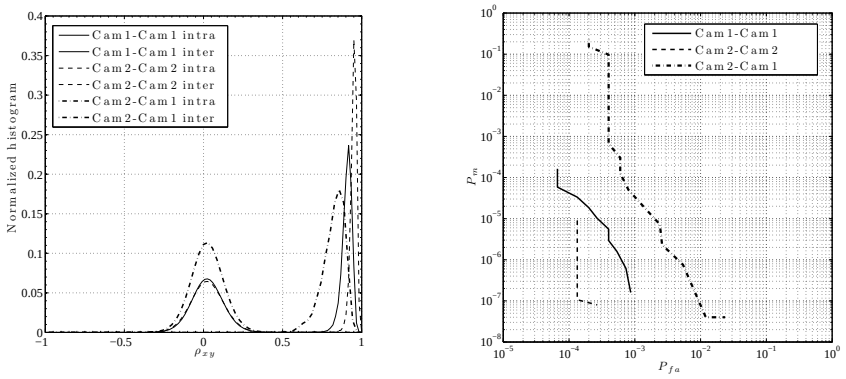
Theoretical bounds and simulations for this authentication architecture can be found in [8]. The *inter* and *intra* class histograms of the correlation coefficients in the random projected domain are shown in Figure 5. To further characterize performance, the ROC curves for the random projection based dimension reduction where $L \in \{64, 256, 1024\}$ using ρ_{xy} as comparison metric are shown in Figure 6. These results lead us

[1] One can also apply special orthogonality techniques to ensure prefect orthogonality.



(a) (b) (c)

Figure 3: The element-wise differences between identical samples in the real domain for all camera combinations with an estimated Gaussian probability density function super imposed.



(a) (b)

Figure 4: The *intra-* and *inter*-class curves and the ROC curves for all cameras using ρ_{xy} in the original domain.

to conclude that reductions to $L = 1024$ lead to performance that is very close to those in the original real domain for all camera combinations. Although dimensionality is significantly reduced, $L \ll N$, the good performance can in part be explained by the fact that the deployed metric is statistically optimal and the L is close to the intrinsic dimension of these microstructure images [9].

V. Binary content fingerprinting

The binarization function $Q(.)$ operates by extracting and storing the sign of all individual elements of all projected data vectors [10]:

$$\begin{aligned}\mathbf{b}_{\mathbf{x}(m)} =&\{sign(\tilde{x}(m)[1]), sign(\tilde{x}(m)[2]),\\ &\ldots, sign(\tilde{x}(m)[L])\},\end{aligned} \tag{10}$$

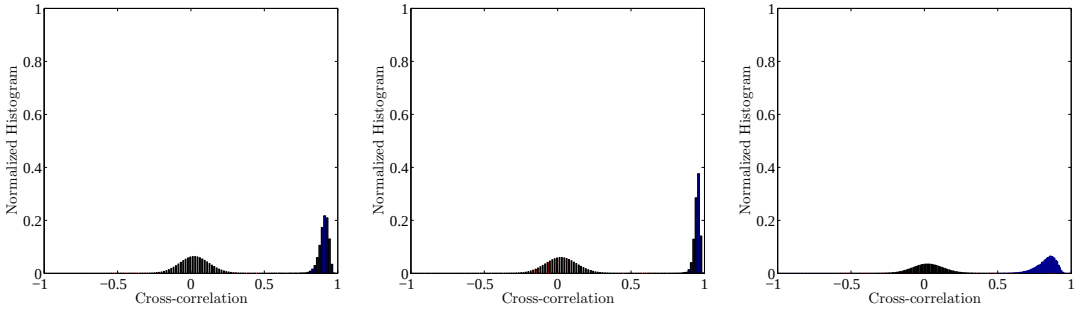
where for $i \in \{1 \ldots L\}$, $b_{\mathbf{x}(m)}[i] \in \{0, 1\}$ and $\forall a, sign(a) = 1$ if $a \geq 0$ and 0 otherwise. Since all projections are almost independent [11], [7], one can assume that the bits in $\mathbf{b}_{\mathbf{x}(m)}$ will be independent and equiprobable for a sufficient large L.[2] This means that the mismatch between the fingerprint of enrolled sample $\mathbf{b}_\mathbf{x}$ and a fingerprint presented for authentication $\mathbf{b}_\mathbf{y}$ can be modelled as a memoryless binary symmetric channel (BSC) with a probability of bit error p_b, where $p_b = \frac{1}{\pi}\arccos(\rho_{\tilde{X}\tilde{Y}})$, where $\arccos(\rho_{\tilde{X}\tilde{Y}})$ is the correlation between $\tilde{X}$ and $\tilde{Y}$ [5].

Based on $\mathbf{B_Y}$ and $\mathbf{B_X}(m)$ a decision criteria based on the Hamming distance, d^H, as sufficient statistic and corresponding binary hypothesis test can be formulated:

$$\begin{cases} H_0 : d^H(\mathbf{b}_\mathbf{y}, \mathbf{b}_\mathbf{x}(m)) > \tilde{\gamma}L, \\ H_m\text{: } d^H(\mathbf{b}_\mathbf{y}, \mathbf{b}_\mathbf{x}(m))) \leq \tilde{\gamma}L, \end{cases} \tag{11}$$

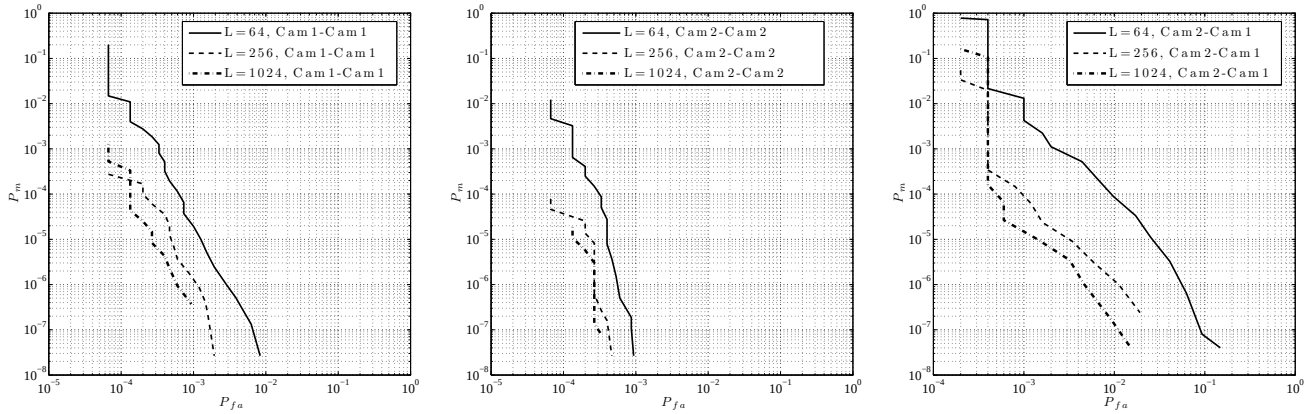
where $\tilde{\gamma}L$ is the threshold controlling the performance of the authentication system The distribution of Hamming distances under hypothesis H_1 follows a Binomial pmf, $\mathcal{B}(L, p_b)$ where p_b represents the probability of bit error between $\mathbf{b}_\mathbf{x}(m)$ and $\mathbf{b}_\mathbf{y}(m)$ under H_1. The distribution of Hamming distances under hypothesis H_0 corresponds to $\mathcal{B}(L, \frac{1}{2})$. The probability of the system falsely rejecting an authentic enrolled item

[2]This assumption can only be made when the input data is independent. Random projected vectors will closely follow a Gaussian pdf but will not necessarily be de-correlated. Deploying Principal Component Analysis (PCA) would not only de-correlate the input vectors, but as the input data is Gaussian, guarantee independence.



(a) Cam1 versus Cam1 (b) Cam2 versus Cam2 (c) Cam1 versus Cam2

Figure 5: The *inter* and *intra* class histograms in the random projection domain for $L = 1024$ using ρ_{xy} as comparison metric.



(a) (b) (c)

Figure 6: ROC curves for all cameras using random projections reducing to $L \in \{64, 256, 1024\}$ dimensions (6a, 6b, 6c) using ρ_{xy} as comparison metric.

therefore is:

$$\begin{aligned} P_m(\tilde{\gamma}) &= Pr[d^H(\mathbf{B_Y}, \mathbf{B_X}(n)) > \tilde{\gamma}L | H_m] \\ &= \sum_{k=\lceil \tilde{\gamma}L \rceil + 1}^{L} \binom{L}{k} p_b^k (1-p_b)^{L-k} \\ &\leq 2^{-LD(\tilde{\gamma}||p_b)}. \end{aligned} \tag{12}$$

where $\mathbf{B_Y}$ is generated from $\mathbf{B_X}(m)$. Conversely, P_{fa}, or the probability that the system will authenticate a non-enrolled or counterfeited item as genuine is:

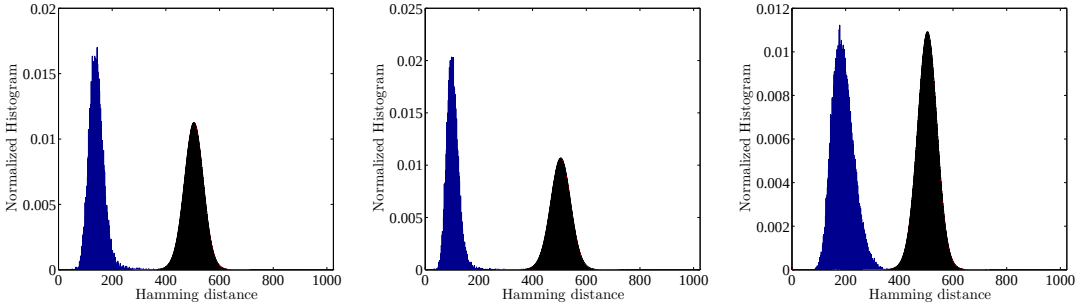
$$\begin{aligned} P_{fa}(\tilde{\gamma}) &= Pr[d^H(\mathbf{B_Y}, \mathbf{B_X})(n) \leq \tilde{\gamma}L | H_0] \\ &= \sum_{k=0}^{\lceil \tilde{\gamma}L \rceil} \binom{L}{k} \frac{1}{2}^k \left(1 - \frac{1}{2}\right)^{L-k} \\ &\leq 2^{-LD(\tilde{\gamma}||\frac{1}{2})}, \\ &= 2^{-L(1-H_2(\tilde{\gamma}))}. \end{aligned} \tag{13}$$

where $\mathbf{B_Y}$ is generated from $\mathbf{B_X}(n)$ and $H_2(.)$ denotes the binary entropy. By selecting the threshold $\tilde{\gamma}L$ one can achieve a trade-off between P_m and P_{fa}. The *inter* and *intra* class Hamming distances are shown in Figure 7 for $L = 1024$ and all camera combinations. These experimental results support the conclusion that the probability of bit error under the hypothesis H_0, where the mean value under H_0 is Lp_b, $p_b \approx \frac{1}{2}$ and that the fingerprint can be considered as independent.

The ROC curves from the experimental results are shown in Figure 8. From this one can conclude that for bit lengths $L = 256$ and $L = 1024$ the binary results closely approximate those of the real valued projected data in Figure 6. The short bit length of $L = 64$, however, causes a sharp drop in performance.

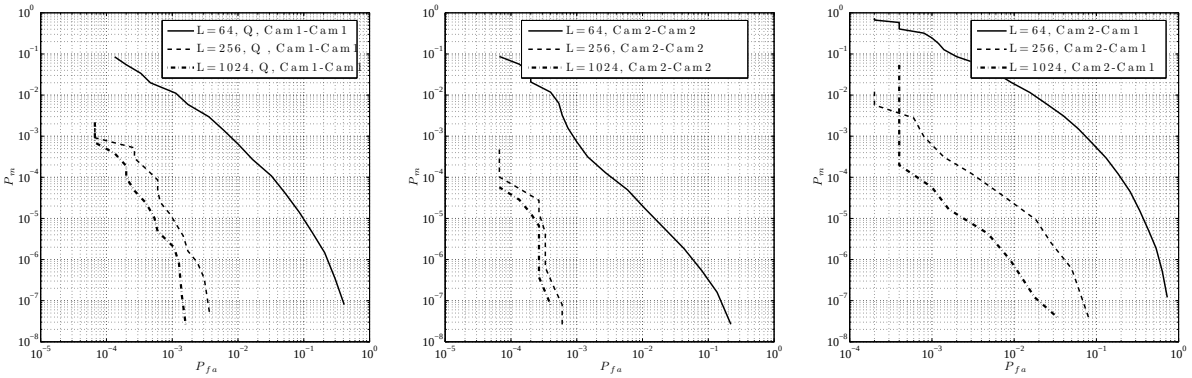
VI. Conclusions

In this paper we have introduced FAMOS, a new publicly available forensic database of micro-structure images for authentication purposes. FAMOS contains 5000 unique samples acquired 3 times with 2 different cameras giving 30000 acquisition samples in total. We have shown the elementary statistical properties of the database and modeled the performance of an authentication framework in the real domain, in the random projected dimension reduced domain and finally in the binary domain for various bit lengths. It is by no means exhaustive in what can be researched with microstructure images and the authors hope to further foster research by the forensic community to develop and test new fingerprinting and identification methods with the help of



(a) Cam1 versus Cam1 (b) Cam2 versus Cam2 (c) Cam1 versus Cam2

Figure 7: The *inter* and *intra* class histograms of the Hamming distance between fingerprints for $L = 1024$.



(a) (b) (c)

Figure 8: ROC curves for all cameras using random projections reducing to $L \in \{64, 256, 1024\}$ dimensions (8a, 8b, 8c), followed by sign based quantization, using the Hamming distance as comparison metric.

this set and the presented base-line performance results. In conclusion, we hope to work towards reproducible results in the domain of physical object protection.

Future work will focus on fingerprinting methods that are resilient against geometrical distortions and the non-linear distortions caused by deploying different cameras and lighting during acquisition. Finally, we have started with the acquisition of new samples from different materials to expand FAMOS with. All code, data and documentation is published on `http://sip.unige.ch/famos`.

VII. Acknowledgments

This work is supported by SNF-grant 20021-132337 and the CRADA project between the University of Geneva and U-NICA systems. Furthermore, the authors would like to thank Markus Rohner for the image acquisition work.

References

[1] A. L. Varna and M. Wu, "Modeling and analysis of correlated binary fingerprints for content identification," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3-2, pp. 1146–1159, 2011.

[2] B. Thomee, M. J. Huiskes, E. Bakker, and M. S. Lew, "Large scale image copy detection evaluation," in *Proceedings of the 1st ACM international conference on Multimedia information retrieval*, ser. MIR '08. New York, NY, USA: ACM, 2008, pp. 59–66. [Online]. Available: http://doi.acm.org/10.1145/1460096.1460108

[3] S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Random projections based item authentication," in *Proceedings of SPIE Photonics West, Electronic Imaging / Media Forensics and Security XI*, San Jose, USA, 2009. [Online]. Available: http://cvml.unige.ch/publications/postscript/2009/2009.SPIE.authentication.rp.pdf

[4] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory (v. 1)*, 1st ed. Prentice Hall, Apr. 1993.

[5] S. Voloshynovskiy, O. Koval, F. Beekhof, F. Farhadzadeh, and T. Holotyak, "Information-theoretical analysis of private content identification," in *IEEE Information Theory Workshop, ITW2010*, Dublin, Ireland, Aug.30-Sep.3 2010.

[6] F. Farhadzadeh, S. Voloshynovskiy, and O. Koval, "Performance analysis of identification system based on order statistics list decoder," in *IEEE International Symposium on Information Theory*, Austin, TX, June, 13-18 2010.

[7] F. Farhadzadeh, S. Voloshynovskiy, O. Koval, T. Holotyak, and F. Beekhof, "Statistical analysis of digital image fingerprinting based on random projections," in *Proceedings of ISPA Image and Signal Processing and Analysis*. ISPA, 2011.

[8] S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Conception and limits of robust perceptual hashing: toward side information assisted hash functions," in *Proceedings of SPIE Photonics West, Electronic Imaging / Media Forensics and Security XI*, San Jose, USA, 2009. [Online]. Available: http://cvml.unige.ch/publications/postscript/2009/2009.SPIE.RPH.limits.pdf

[9] W. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," vol. 26, pp. 189–206, 1984.

[10] A. Gionis, P. Indyk, and R. Motwani, "Similarity search in high dimensions via hashing," pp. 518–529, 1999.

[11] F. Farhadzadeh, S. Voloshynovskiy, and O. Koval, "Performance analysis of content-based identification using constrained list-based decoding," *IEEE Trans. on Forensic and information security*, 2012.