Physical object authentication with correlated camera noise

F. P. Beekhof, S. Voloshynovskiy, M. Diephuis, F. Farhadzadeh

CUI
University of Geneva
route de Drize 7
1227 Carouge
svolos@unige.ch

Abstract: In this paper, we address the problem of physical object authentication based on surface microstructure images. The authentication is based on digital content fingerprints computed from the microstructure images. We analyze the impact of camera distortions which follow additive correlated Gaussian noise. The optimal decision rule is derived and the performance is analyzed in the direct and transformed domain. The theoretical derivations are supported by experimental results obtained for the FAMOS dataset.

1 Introduction

Counterfeit products are increasingly present in the market, leading to a number of issues for legitimate manufacturers and consumers alike. Although manufacturers might be primarily interested in preventing any loss of income, the well-being of consumers can be seriously affected by counterfeit products such as car brakes or medication.

Although solutions exist where original items or their packaging are modified, such as by attaching holograms or embedding a digital watermark, a recent development has been to base protection systems on forensic features that require no modification of the items. Forensic techniques are based on the intrinsic features of the objects to be protected. A particularly attractive option is the use of microstructures, which can be acquired by commonly available optical equipment. Microstructures have been shown to be present in almost all materials and to be robust against rough treatment of the material [BCJ$^+$05].

Although the use of microstructures is an attractive option, their usage directly entails a number of drawbacks, most notably the large storage space required, concerns about the safety of the stored data, and the effort required to process the data during queries. A solution to these concerns exists in the form of *digital content fingerprints*, which are short, robust and informative representations of these images.

A similar approach is taken in the field of biometrics [TSE07, Ign09], where noisy data acquired from a person is transformed into a binary *template*, which must be protected due to the great importance of privacy in biometric applications. Due to the fact that microstructures are acquired in the form of images, there is a strong link with multimedia security, and particularly robust image hashing [BL96, Fri00, FLL02, SMW06].

Fingerprints are typically stored in conjuction with an identifier, usually the index in a table of fingerprints, in a relational database. In this context it is clear that the identifier is a primary key in the database. Note that a *key* in the context of this work refers to a database key, not a secret key as used in cryptography, biometrics or multimedia security. Although the identifier is a valid database key, the fingerprint should satisfy many of the same constraints, namely, a fingerprint always has a value and is expected to be uniquely associated with the item it is derived from. A difference between traditional database keys is that fingerprints are random, determined by the natural randomness of the items from which they are derived and partially by noise. This implies several differences with traditional database keys. First, the uniqueness of fingerprints is not guaranteed, whereas a simple automatic increment is sufficient to guarantee the uniqueness of traditional database keys. Second, the fingerprints calculated from different observations of the same item differ slightly due to the noise. This can be likened to executing database operations on a machine where data are corrupted due to failing memory modules. The presence of noise has two very serious consequences: first, the time-complexity of a database lookup increases from $O(1)$ to exponential in the fingerprint length; second, the lookup might return an erroneous result due to the fact that the introduced uncertainty renders it impossible to confirm that a match in correct.

The problem wherein the identity of the item under investigation is established by matching a query fingerprint against the full database of fingerprints, is refered to as the identification problem. In this work, we address a simpler case, the authentication problem, which only establishes if an unknown item is in fact a specific item in the database indicated by the user. This can be seen as a query with a fingerprint against one specific row of the fingerprint table in the database, or against a table with one row. In this work we will investigate the probability of error of a query based on fingerprints in the authentication setup, and propose improved matching rules to decrease that probability of error.

In previous work, the authors have released *FAMOS* [VDB$^+$12], a forensics dataset of images of microstructure of cardboard boxes, and made several theoretical and practical contributions to the field of fingerprinting [Bee12].

Although significant progress has been made in the field, there is still room for improvement of the fingerprinting technology in terms of robustness and the precision of matching. In this work, we propose enhanced observation models of the noise, and corresponding rules for the matching of observations and fingerprints, leading to improved performance.

1.1 Notation

Bold capitals $\mathbf{X}$ denote vector random variables. Corresponding small letters $\mathbf{x}$ denote their respective realizations. The binarized version of $\mathbf{x}$ is represented by $\mathbf{b_x}$. $\mathbf{X} \sim f(\mathbf{x})$ indicates that the random vector follows distribution $f(\mathbf{x})$. The identity matrix is denoted as $\mathbb{I}$.

2 Model of Authentication

Although other solutions exist, physical objects can be protected against counterfeiting through authentication services, which determine if a particular object is truly the authentic object m that it is claimed to be.

An overview of authentication for physical objects is given in Figure 1. There are two phases in the authentication system: *enrollment*, where authentic items are produced and their fingerprints are placed in a database; followed by *verification*, wherein it is claimed that an unknown object is the authentic object with identify m, and it must be decided if this is true or not. During the enrollment, an image of the microstructure of an authentic object, which is given an identity m, is acquired. The image obtained from item m is represented by the vector $\mathbf{x}(m)$, which is transformed into a fingerprint $\mathbf{b}_{\mathbf{x}}(m)$. The fingerprint is then stored in a database.

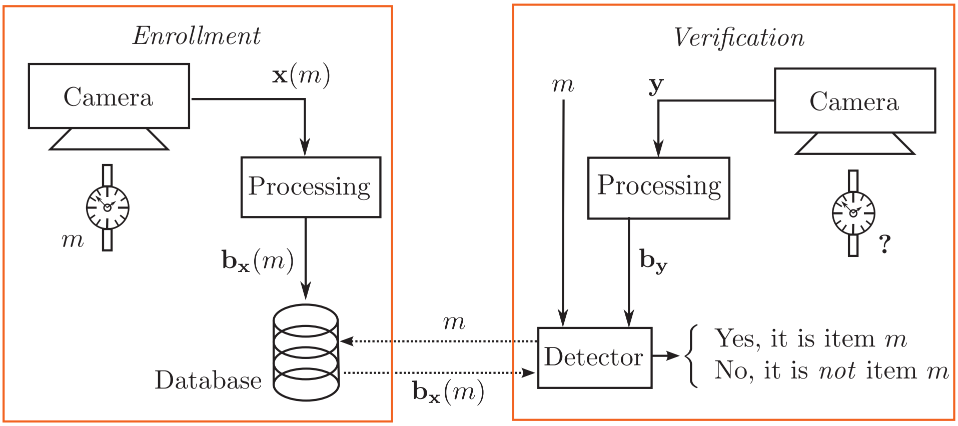


Figure 1: An authentication scheme based on fingerprinting of microstructures.

During verification, the noisy data $\mathbf{y}$, acquired from the object under investigation, is used to calculate a fingerprint $\mathbf{b}_{\mathbf{y}}$. The claimed identity m is used to retrieve $\mathbf{b}_{\mathbf{x}}(m)$, the content fingerprint of the authentic object m, from the database. The decision about the authenticity of the object under verification is then made by comparing $\mathbf{b}_{\mathbf{x}}(m)$ with $\mathbf{b}_{\mathbf{y}}$.

We can then formulate the authentication problem as a binary hypothesis test to answer the question whether or not the observed item is the authentic item m, i.e.:

$$\begin{cases} \mathcal{H}_0 : \text{No, it is } \textit{not} \text{ the authentic item } m, \\ \mathcal{H}_m : \text{Yes, it is the authentic item } m. \end{cases} \tag{1}$$

2.1 Mathematical formulation of Authentication

The process shown in Figure 1 can be expressed mathematically as shown in Figure 2, which details the calculation of the fingerprint. During the enrollment stage, a source $\mathbf{X}$ generates a vector of features associated with m, the identity of the object, resulting in a realisation denoted as $\mathbf{x}(m)$. The calculation of the fingerprint is modeled as a two-step process: in the first stage, the data is transformed by a matrix $\mathbf{W}$, producing $\tilde{\mathbf{X}}(m)$, which can be quantized by a function Q to produce the fingerprint $\mathbf{B}_{\mathbf{X}}(m)$.

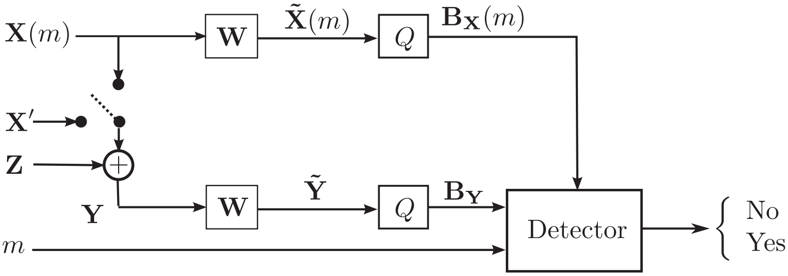


Figure 2: Mathematical overview of authentication based on content fingerprinting.

During verification, either the authentic object $\mathbf{x}(m)$ is observed, or any other item denoted as $\mathbf{X}'$. We assume that $\mathbf{X}'$ is generated from the same source that produced $\mathbf{x}(m)$. We assume that the counterfeiters have the same equipment or the technological details of the manufacturing process. However, we assume that they can not control the physical randomness of microstructures, which is a strong assumption. Mathematically, this can be expressed by assuming that counterfeiters can produce counterfeit items $\mathbf{X}'$ such that $\mathbf{X}' \sim f(\mathbf{X})$. The acquisition during verification may introduce additive noise $\mathbf{Z}$ that is independent of the item under investigation, producing a vector $\mathbf{Y}$. The noisy vector $\mathbf{Y}$ is transformed using $\mathbf{W}$ and quantized by Q, producing $\mathbf{B}_{\mathbf{Y}}$.

We will investigate the authentication problem in the direct and transformed domains. In the *direct* domain, the data evaluated directly, i.e. the data is not modified. In the *transformed* domain, the data first undergoes a transformation, represented by $\mathbf{W}$ in Figure 2, and the transformed data is evaluated.

2.2 Direct Domain

In mathematical terms, we can reformulate the hypothesis test in the direct domain as:

$$\begin{cases} \mathcal{H}_0 : \mathbf{Y} = \mathbf{X}' + \mathbf{Z}, \\ \mathcal{H}_m : \mathbf{Y} = \mathbf{x}(m) + \mathbf{Z}. \end{cases} \tag{2}$$

In previous work [VKP08, VDB$^+$12, Bee12], it was assumed that both the source $\mathbf{X}$ and the noise were $\mathbf{Z}$ are i.i.d. Gaussian, from which it follows that the correlation is a sufficient statistic in the direct domain. In this work, we relax these assumptions and allow for correlated noise, i.e., we assume that $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{xx})$ and $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{zz})$. We make no assumptions about the counterfeit items $\mathbf{X}'$ other than that they are generated from the same distribution as authentic items. Consequently, the hypothesis test can be reformulated in terms of the distributions:

$$\begin{cases} \mathcal{H}_0 : \mathbf{Y} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{xx} + \mathbf{K}_{zz}), \\ \mathcal{H}_m : \mathbf{Y} \sim \mathcal{N}(\mathbf{x}(m), \mathbf{K}_{zz}). \end{cases} \tag{3}$$

Following the Neyman-Pearson framework, we can then formulate the decision rule for a chosen threshold γ which can be developed using Bayes' rule:

$$\frac{\Pr[\mathcal{H}_m \mid \mathbf{y}]}{\Pr[\mathcal{H}_0 \mid \mathbf{y}]} > \gamma \qquad \Leftrightarrow \qquad \frac{\frac{f(\mathbf{y}|\mathcal{H}_m)p(\mathcal{H}_m)}{f(\mathbf{y})}}{\frac{f(\mathbf{y}|\mathcal{H}_0)p(\mathcal{H}_0)}{f(\mathbf{y})}} > \gamma. \tag{4}$$

Assuming $p(\mathcal{H}_0) = p(\mathcal{H}_m) = \frac{1}{2}$, which implies the greatest uncertainty about the hypothesis in force, yields:

$$\frac{f(\mathbf{y} \mid \mathcal{H}_m)}{f(\mathbf{y} \mid \mathcal{H}_0)} > \gamma \tag{5}$$

$$\frac{\frac{1}{\sqrt[N]{2\pi}\sqrt{|\mathbf{K}_{zz}|}} \exp\left(-\frac{1}{2}(\mathbf{y} - \mathbf{x}(m))^T \mathbf{K}_{zz}^{-1}(\mathbf{y} - \mathbf{x}(m))\right)}{\frac{1}{\sqrt[N]{2\pi}\sqrt{|(\mathbf{K}_{xx}+\mathbf{K}_{zz})|}} \exp\left(-\frac{1}{2}\mathbf{y}^T(\mathbf{K}_{xx} + \mathbf{K}_{zz})^{-1}\mathbf{y}\right)} > \gamma, \tag{6}$$

where $|.|$ denotes the determinant of the matrix, and which can be further developed to obtain a sufficient statistic [Kay98]:

$$t(\mathbf{y}) = \mathbf{y}^T(\mathbf{K}_{xx} + \mathbf{K}_{zz})^{-1}\mathbf{y} - (\mathbf{y} - \mathbf{x}(m))^T \mathbf{K}_{zz}^{-1}(\mathbf{y} - \mathbf{x}(m)) \tag{7}$$

$$= \mathbf{y}^T(\mathbf{K}_{xx} + \mathbf{K}_{zz})^{-1}\mathbf{y} - \mathbf{y}^T\mathbf{K}_{zz}^{-1}\mathbf{y} + 2\mathbf{y}^T\mathbf{K}_{zz}^{-1}\mathbf{x}(m) - \mathbf{x}^T(m)\mathbf{K}_{zz}^{-1}\mathbf{x}(m). \tag{8}$$

A simplified sufficient statistic $s(\mathbf{y})$ can be formulated by assuming that the terms $\mathbf{y}^T(\mathbf{K}_{xx} + \mathbf{K}_{zz})^{-1}\mathbf{y}$, $\mathbf{y}^T\mathbf{K}_{zz}^{-1}\mathbf{y}$ and $\mathbf{x}^T(m)\mathbf{K}_{zz}^{-1}\mathbf{x}(m)$ are all constant for the expected observations:

$$s(\mathbf{y}) = \mathbf{y}^T\mathbf{K}_{zz}^{-1}\mathbf{x}(m). \tag{9}$$

2.3 Transformed Domain

The calculation of a fingerprint typically involves a transformation, which we assume to be linear and orthogonal. An example of such a transform is the DCT, but random projections, which are approximately orthogonal [VKB$^+$10, FVK10] can be considered as well. Let

$$\tilde{\mathbf{X}} = \mathbf{W}\mathbf{X}, \quad \tilde{\mathbf{Y}} = \mathbf{W}\mathbf{Y}, \quad \text{and } \tilde{\mathbf{Z}} = \mathbf{W}\mathbf{Z}, \tag{10}$$

then

$$\tilde{\mathbf{Y}} = \mathbf{W}\mathbf{Y} = \mathbf{W}(\mathbf{X} + \mathbf{Z}) = \mathbf{W}\mathbf{X} + \mathbf{W}\mathbf{Z} = \tilde{\mathbf{X}} + \tilde{\mathbf{Z}}, \tag{11}$$

where $\tilde{\mathbf{X}} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\tilde{x}\tilde{x}})$, $\tilde{\mathbf{Z}} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\tilde{Z}\tilde{Z}})$, and $\mathbf{K}_{\tilde{x}\tilde{x}} = \mathbf{W}\mathbf{K}_{\tilde{x}\tilde{x}}\mathbf{W}^T$ and $\mathbf{K}_{\tilde{z}\tilde{z}} = \mathbf{W}\mathbf{K}_{\tilde{z}\tilde{z}}\mathbf{W}^T$ [Jai89]. The hypothesis test in the transformed domain is then:

$$\begin{cases} \mathcal{H}_0 : \tilde{\mathbf{Y}} = \tilde{\mathbf{X}}' + \tilde{\mathbf{Z}}, \\ \mathcal{H}_m : \tilde{\mathbf{Y}} = \tilde{\mathbf{x}}(m) + \tilde{\mathbf{Z}}, \end{cases} \tag{12}$$

which can be reformulated as in the direct domain:

$$\begin{cases} \mathcal{H}_0 : \tilde{\mathbf{Y}} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\tilde{x}\tilde{x}} + \mathbf{K}_{\tilde{z}\tilde{z}}), \\ \mathcal{H}_m : \tilde{\mathbf{Y}} \sim \mathcal{N}(\tilde{\mathbf{x}}(m), \mathbf{K}_{\tilde{z}\tilde{z}}), \end{cases} \tag{13}$$

leading to a sufficient statistic in the transformed domain:

$$s(\tilde{\mathbf{y}}) = \tilde{\mathbf{y}}^T \mathbf{K}_{\tilde{z}\tilde{z}}^{-1} \tilde{\mathbf{x}}(m). \tag{14}$$

The challenge for systems designers is to choose a transform that leads to the most informative and robust fingerprints, which can be evaluated in information-theoretical terms, using the framework introduced in earlier work [Bee12].

3 Experimental Results

In this work, we have opted to use the DCT as transform because of its energy-compacting properties, which offer a good future perspective for dimensionality reduction.

As stated earlier, the statistic derived for i.i.d. Gaussian noise is the sum-inner-product, both in the direct and in the transformed domain [VKP08]:

$$r(\mathbf{y}) = \mathbf{y}^T \mathbf{x}(m), \quad r(\tilde{\mathbf{y}}) = \tilde{\mathbf{y}}^T \tilde{\mathbf{x}}(m). \tag{15}$$

There are two sources of error in authentication: first, an item that is *not* item m may nonetheless be accepted as such; second, the authentic item m may be wrongfully rejected. The latter case is refered to as a *miss*.

Let the probability of miss p_m, and false acceptance p_f be defined for each of the different statistics as:

$$p_m = \Pr\left[r(\mathbf{Y}) < t \mid \mathcal{H}_m\right] \qquad p_f = \Pr\left[r(\mathbf{Y}) \geq t \mid \mathcal{H}_0\right], \tag{16}$$

$$p_m = \Pr\left[r(\tilde{\mathbf{Y}}) < t \mid \mathcal{H}_m\right] \qquad p_f = \Pr\left[r(\tilde{\mathbf{Y}}) \geq t \mid \mathcal{H}_0\right], \tag{17}$$

$$p_m = \Pr\left[s(\mathbf{Y}) < t \mid \mathcal{H}_m\right] \qquad p_f = \Pr\left[s(\mathbf{Y}) \geq t \mid \mathcal{H}_0\right], \tag{18}$$

$$p_m = \Pr\left[s(\tilde{\mathbf{Y}}) < t \mid \mathcal{H}_m\right] \qquad p_f = \Pr\left[s(\tilde{\mathbf{Y}}) \geq t \mid \mathcal{H}_0\right], \tag{19}$$

where t is a threshold that must be derived from the chosen threshold γ for each statistic. The authentication performance will be analysed in terms of a Receiver Operating Characteristic (ROC) curve.

3.1 Authentication Performance on Synthetic Data

The performance has first been evaluated for synthetic data, where $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, \mathbb{I})$ and $\mathbf{Z}$ was generated by a stationary Gauss-Markov process with $\rho_Z = 0.85$, i.e. $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{zz})$. The length of the vectors was 128, and 4096 different vectors were enrolled, then transformed with a one-dimensional DCT. The results are visible in Figure 5a, indicating in all cases that the use of the proposed measures $s(\mathbf{y})$ and $s(\tilde{\mathbf{y}})$ lead to greater precision than the use of regular inner products $r(\mathbf{y})$ and $r(\tilde{\mathbf{y}})$. It also demonstrated that there is no difference between the direct domain and the transformed domain. The transform does not alter the performance, i.e. the performance of $r(\mathbf{y})$ and $r(\tilde{\mathbf{y}})$ are similar, and the same holds for the performance of $s(\mathbf{y})$ and $s(\tilde{\mathbf{y}})$.

3.2 Authentication Performance on the FAMOS dataset

The FAMOS[1] dataset contains images of 5000 cardboard patches acquired with two different cameras [VDB$^+$12]. Each cardboard patch is acquired three times with the same camera, resulting in acquisitions A, B and C and a total of 30000 images. Examples of these acquisitions can be seen in Figure 3.

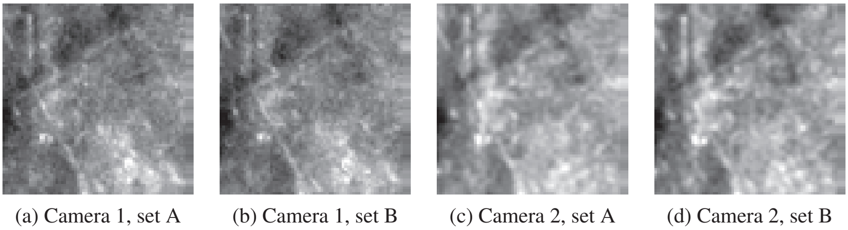

(a) Camera 1, set A (b) Camera 1, set B (c) Camera 2, set A (d) Camera 2, set B

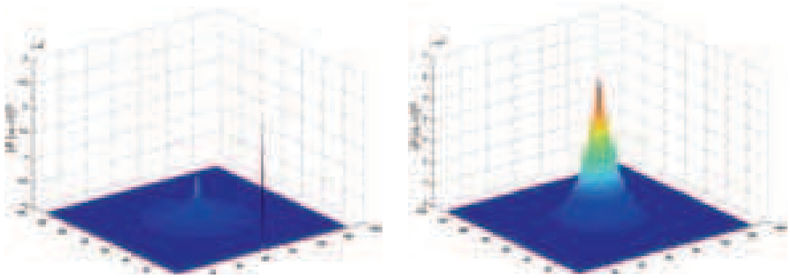
Figure 3: Multiple acquisitions of a single microstructure sample. Histogram equalization was used for visualisation purposes.

A justification for the assumption of correlated noise can be seen in Figure 4, where the spectra of the differences between acquisition images of an identical sample are shown. The non-uniformity of the spectra confirms the dominance of low frequencies, indicating a correlation between the elements of the noise.

In these experiments, the acquisition sets A and B were compared for both cameras to produce the results. The images have been pre-processed to render them zero-mean and unit variance to compensate for any variations in the lighting conditions, which could result in potentially varying means and dynamic ranges. The inner product $r(\mathbf{y})$ is therefore mathematically identical to the sample cross-correlation.

Figure 5b shows the results for when the camera 1 is used for both enrollment and verifica-

[1] http://sip.unige.ch/famos



(a) Camera 1

(b) Camera 2

Figure 4: Spectra of the noise showing correlation in the noise of the FAMOS dataset.

tion, whereas Figure 5c corresponds to the case where camera 2 is used for both enrollment and verification. The curves for $s(\mathbf{y})$ and $s(\tilde{\mathbf{y}})$ are absent in Figures 5b and 5c, which indicates that either p_m or p_f can be reduced to zero when the same camera is used for enrollment and verification when using the proposed statistics.

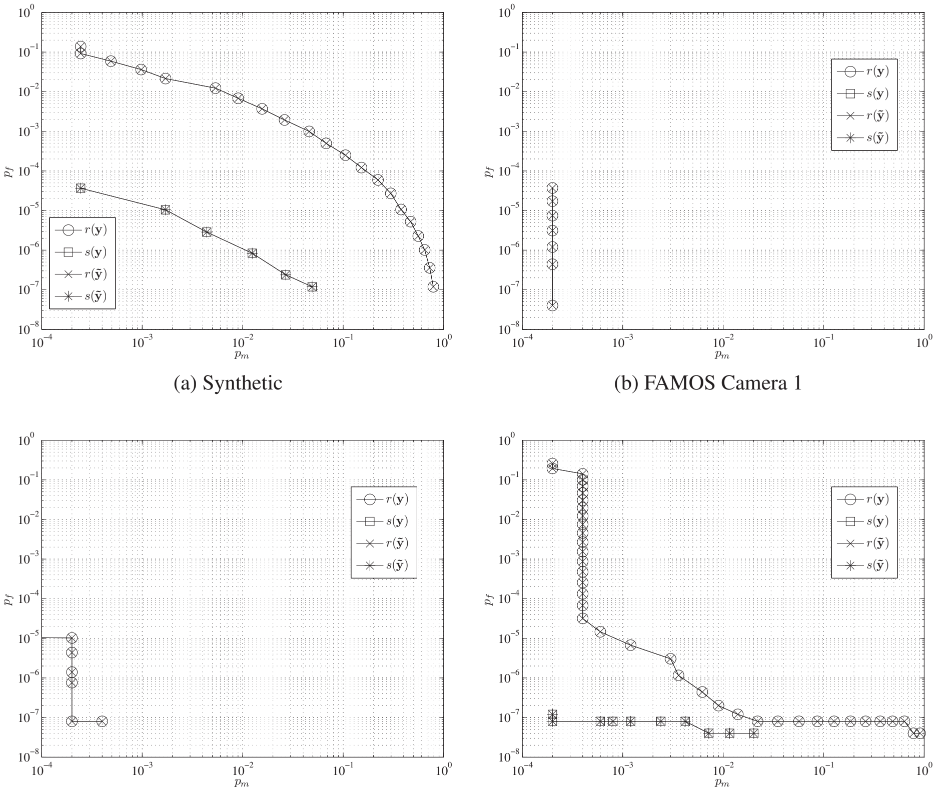
Figure 5d shows results for the case where camera 1 is used for enrollment, and camera 2 for verification. In this case, the performance is relatively decreased relative to the case where only one camera is involved, as can be seen from the corresponding ROC curves.

In all cases, the fact remains that deploying the proposed sufficient statistics $s(\mathbf{y})$ and $s(\tilde{\mathbf{y}})$ leads to a significant performance improvement over $r(\mathbf{y})$ and $r(\tilde{\mathbf{y}})$, respectively. Additionally, we see that the chosen transform does not impact the performance, neither for synthetic data or the true microstructure images from the FAMOS dataset.

4 Conclusions

In this work we have shown that a sufficient statistic based on a model with correlated noise leads to significantly better performance, on both synthetic data and on true microstructure images from the FAMOS dataset, in comparison to sufficient statistics for the case of i.i.d. additive white Gaussian noise.

There are a significant number of directions for future research. First, an important aspect of content fingerprinting that has not been addressed in this work is dimensionality reduction, which can be optimized with respect to robustness against distortions. Second, the role of quantization and sufficient statistics in the binary domain are of vital importance, as fingerprints are usually binary sequences. Third, the development and testing of improved matching techniques, specifically matching real the transformed data against binary fingerprints, can be explored. Fourth, the performance can most likely be improved even further by reconstructing $\tilde{\mathbf{X}}$ from a binary fingerprint and other information available at the detector. Furthermore, we aim to develop a thorough information-theoretical analysis based on the framework introduced in [Bee12]. Last, the results can be extented to the identification setup.



(a) Synthetic

(b) FAMOS Camera 1

(c) FAMOS Camera 2

(d) FAMOS Camera 1 vs 2

Figure 5: ROC curves of authentication on synthetic data and the FAMOS datasets.

Acknowledgment

This work is supported by SNF-grant 20021-132337 and the CRADA project between the University of Geneva and U-NICA systems.

References

[BCJ+05] James D. R. Buchanan, Russell P. Cowburn, Ana-Vanessa Jausovec, Dorothee Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A. Allwood, and Matthew T. Bryan. Forgery: 'Fingerprinting' documents and packaging. *Nature*, 436(7050):475–475, 2005.

[Bee12] Fokko Beekhof. *Physical Object Protection based on Digital Micro-structure Fingerprinting*. PhD thesis, University of Geneva, 2012.

[BL96] Robert D. Brandt and Feng Lin. Representations that uniquely characterize images modulo translation, rotation, and scaling. *Pattern Recognition Letters*, 17:1001–1015, 1996.

[FLL02] Benoit Macq Frèdèric Lefèbvre and Jean-Didier Legat. Radon soft hash algorithm. In *Proceedings of the European Signal Processing Conference*, Toulouse, France, September 2002.

[Fri00] J. Fridrich. Visual hash for oblivious watermarking. In P. W. Wong and E. J. Delp, editors, *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, volume 3971 of *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, pages 286–294, May 2000.

[FVK10] Farzad Farhadzadeh, Sviatoslav Voloshynovskiy, and Oleksiy 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.

[Ign09] Tanya Ignatenko. *Secret-Key Rates and Privacy Leakage in Biometric Systems*. PhD thesis, Technical University of Eindhoven, 2009.

[Jai89] Anil K. Jain. *Fundamentals of Digital Image Processing*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989.

[Kay98] Stephen Kay. *Fundamentals of Statistical Signal Processing, Vol II - Detection Theory*. Prentice-Hall, Inc., 1998.

[SMW06] Ashwin Swaminathan, Yinian Mao, and Min Wu. Robust and secure image hashing. *Information Forensics and Security, IEEE Transactions on*, 1(2):215 – 230, June 2006.

[TSE07] Pim Tuyls, Boris Skoric, and Tom Kevenaar (Eds.). *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer, 2007.

[VDB$^+$12] Sviatoslav Voloshynovskiy, Maurits Diephuis, Fokko Beekhof, Oleksiy Koval, and Bruno Keel. Towards Reproducible results in authentication based on physical noncloneable functions: The Forensic Authentication Microstructure Optical Set (FAMOS). In *Proceedings of IEEE International Workshop on Information Forensics and Security*, Tenerife, Spain, December 2–5 2012.

[VKB$^+$10] 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, August 30 – September 3 2010.

[VKP08] Sviatoslav Voloshynovskiy, Oleksiy Koval, and Thierry Pun. Multimodal authentication based on random projections and distributed coding. In *Proceedings of the 10th ACM Workshop on Multimedia & Security*, Oxford, UK, September 22–23 2008.