Statistical Analysis of Digital Image Fingerprinting Based on Random Projections

Farzad Farhadzadeh, Sviatoslav Voloshynovskiy, Oleksiy Koval, Taras Holotyak and Fokko Beekhof

Computer Science Department
University of Geneva
7 route de Drize, CH 1227, Geneva, Switzerland
Email: {Farzad.Farhadzadeh, svolos, Oleksiy.Koval, Taras.Holotyak, Fokko.Beekhof}@unige.ch

***Abstract*—Digital fingerprints have recently received a lot of interest in multimedia applications due to their low dimensionality and security/privacy preserving capabilities. In digital fingerprint extraction, random projections play an important role due to their approximate distance preserving property. This paper is dedicated to the analysis of the statistical properties of digital fingerprints obtained based on random projections. In particular, we were able to demonstrate that this sort of mapping guarantees approximate decorrelation of its output with high probability.**

I. Introduction

In recent years, many multimedia applications such as content based retrieval, content filtering and automatic tagging, content based identification and authentication, and biometrics are using high dimensional multimedia data, that are frequently privacy-sensitive. There exist several approaches to deal with these problems, such as robust hashing or digital fingerprinting. A *digital fingerprint* represents a short, robust and distinctive content description, allowing fast operations.

Multimedia management and security applications based on digital fingerprinting have received a lot of interest in the research community and several different approaches for digital fingerprinting have been proposed. In most cases, digital fingerprinting consists of a dimensionality reduction by applying some content independent transform and binarization [1], [2], [3]. For security/privacy reasons, this transform can also be key-dependent. The main idea behind digital fingerprinting approaches is to extract digital fingerprints of a lower dimensionality with a maximum possible entropy. For instance, in the binary case one expects the bits of digital fingerprints to be independently and equally likely 0s and 1s. Since multimedia data are correlated, one of the principle tasks of the dimensionality reduction transform is to eliminate the correlation between their samples.

The optimal mapper that possesses such properties is the Karhunen-Loève transform (KLT) [4]. This transform perfectly decorrelates data as well as optimally compacts their energy into fewer amount of elements, making dimensionality reduction straightforward. However, the price to pay for this optimality is its data dependence and high computational complexity. The latter issue gains importance due to the fact that computational complexity of this transform can be evaluated as $\mathcal{O}(N^3)$, where N is the dimensionality of its input [5]. Besides the above drawbacks, the necessity to share the basis vectors for the decoding stage makes this transform unpractical in the privacy-sensitive applications.

In order to relax this dependence, several approximations of the KLT were proposed. These include, for example, the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [4], which demonstrate a nearly optimal decorrelation of locally correlated data. The basis vectors of these transforms are fixed and independent of the statistics of their inputs. Due to their decorrelation and energy compaction capabilities as well as the existence of fast implementation algorithms, they are a common tool in various signal and image processing applications. However, similarly to the KLT the main drawback of such fixed basis transforms consists in the public disclosure of the basis vectors, which could be unacceptable for multimedia security applications [6].

One solution to overcome this privacy/security shortcoming is a randomized mapper that can be designed based on random projections (RP) [2]. The RP have been the object of much interest due to their ability to preserve distance between vectors after embedding into a lower dimensional space that has also recently been recognized in the Compressed Sensing community for sparse data [7], [8]. Moreover, by applying the RP one can convert an unknown distribution of original data to Gaussian [9]. However, in multimedia applications, data are correlated. Although the decorrelation property of orthogonal transforms is well-known [4], the RP are based on approximately orthogonal bases. The statistics of projected data, e.g., the covariance matrix, are not well justified. On the other hand, prior knowledge of the statistics of extracted digital fingerprints to evaluate the performance of content based identification and retrieval systems is mandatory.

Therefore, the main goal of this paper is to investigate the statistical properties of digital fingerprints based on the RP for different classes of image models that include either independent and identically distributed (i.i.d.) models with a symmetric Probability Density Function (PDF), which models the output coefficients of the DCT or DWT, or correlation-based models like the Gauss-Markov processes, which capture image pixel dependencies directly in the coordinate domain [4]. At our best knowledge, this problem was not addressed yet by the research community in the current formulation. The analysis in

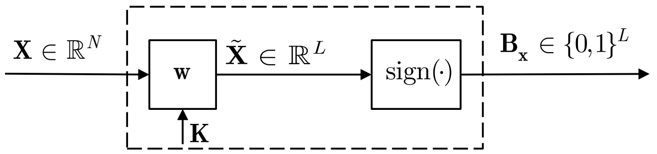

$\mathbf{X} \in \mathbb{R}^N$
$\mathbf{w}$
$\tilde{\mathbf{X}} \in \mathbb{R}^L$
$\mathrm{sign}(\cdot)$
$\mathbf{B}_{\mathrm{x}} \in \{0{,}1\}^L$
$\mathbf{K}$

Fig. 1. Digital fingerprint extraction.

[10] was focus rather on the performance analysis of forensic fingerprinting based on i.i.d./ correlated fingerprints than on the statistical analysis of fingerprint generating model.

The outline of the paper is as follows. Section II contains a statistical analysis of data correlation in the RP domain. Experimental validation of our theoretical results is presented in Section III. Finally, Section IV concludes the paper.

Notations: We use capital letters X to denote scalar random variables and $\mathbf{X}$ to denote vector random variables. Corresponding small letters x and $\mathbf{x}$ denote the realizations of scalar and vector random variables, respectively. All vectors without sign tilde are assumed to be of length N and with the sign tilde of length L, i.e., $\mathbf{x} = \{x_1, x_2, \dots, x_N\}$ and $\tilde{\mathbf{x}} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_L\}$, where $x_i, \tilde{x}_j$ are elements of $\mathbf{x}$ and $\tilde{\mathbf{x}}$, respectively $(1 \le i \le N, 1 \le j \le L)$. Bernoulli$(p)$ indicates the Bernoulli distribution with the probability of success p. $\mathcal{B}(N,p)$ denotes the Binomial distribution with N trails and probability of success p. $E[\cdot]$ designates the expectation.

II. Statistical Analysis

This Section is dedicated to the statistical analysis of extracted digital fingerprints using the RP and binarization. Digital fingerprint extraction, which is illustrated in Fig. 1, consists of two following steps: *Dimensionality reduction* and *Binarization*. At the dimensionality reduction stage, the dimensionality of data $\mathbf{X}$ is reduced from N to L, $L \le N$, by applying the RP, which are approximately *orthoprojectors*, i.e., $\mathbf{w}\mathbf{w}^T \approx \mathbf{I}_L$, where $\mathbf{w} \in \frac{1}{\sqrt{N}}\{\pm 1\}^{L \times N}$ with elements $W_{ij} \sim$ Bernoulli$(\frac{1}{2})$, $1 \le i \le L$ and $1 \le j \le N$. The transform $\mathbf{W}$ can also be generated using some secret key $\mathbf{K}$. At the binarization stage, L-length binary data are derived from the projected data elements by taking the sign of the projected data, i.e., $\mathbf{B}_{\mathbf{x}} = \{\mathrm{sign}(\tilde{X_1}), \dots, \mathrm{sign}(\tilde{X_L})\}, \mathrm{sign}(x) = \begin{cases} 1, x > 0 \\ 0, x \le 0 \end{cases}$, where $\tilde{\mathbf{X}} = \mathbf{w}\mathbf{X}$ for a given $\mathbf{w}$.

A. Correlated Data Analysis

In this Section, we investigate the statistics of digital fingerprints obtained by applying the RP in the coordinate domain. We assume that the data $\mathbf{X}$ are real zero-mean random vectors modeled as the Gauss-Markov process. This is a simple but often-used model in image processing [4]. For a given $\mathbf{w}$, one has:

$$\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} = E[\mathbf{w}\mathbf{X}\mathbf{X}^T\mathbf{w}^T] = \mathbf{w}\mathbf{K}_{\mathbf{x}\mathbf{x}}\mathbf{w}^T, \tag{1}$$

where $\mathbf{K}_{\mathbf{x}\mathbf{x}}$ is defined by [4]:

$$\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} = \sigma_X^2 \begin{bmatrix} 1 & \rho & \dots \rho^{N-1} \\ \rho & 1 & \dots \rho^{N-2} \\ \vdots & \vdots & \ddots \ \vdots \\ \rho^{N-1} & \rho^{N-2} & \dots \ 1 \end{bmatrix}, \tag{2}$$

where ρ is the normalized correlation coefficient. We prove the following proposition for statistical modeling of projected data.

Proposition 1 (Decorrelation property of RP). Let the elements of the RP matrix, $\mathbf{w}$ of size $L \times N$ and $1 < L \le N$, be drawn from the probability mass function (PMF) $\Pr\{W_{ij} = +\frac{1}{\sqrt{N}}\} = \Pr\{W_{ij} = -\frac{1}{\sqrt{N}}\} = \frac{1}{2}$, and $\mathbf{X}$ be a real zero-mean random vector modeled as the Gauss-Markov process with variance σ_X^2 and normalized correlation coefficient ρ. Then, we have:

$$\Pr\left\{\max_{i \ne j} |\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ij}| > \beta\sigma_X^2\right\} < \frac{1}{L}, \tag{3a}$$

$$\Pr\left\{\max_{i} |\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ii} - \sigma_X^2| > \alpha\sigma_X^2\right\} < \frac{2}{L^{(\frac{1}{\rho})}}, \tag{3b}$$

where $\beta = \sqrt{\frac{12}{N}\left(\frac{1-\rho^N}{1-\rho}\right)^2 \ln L}$, $\alpha = \sqrt{\frac{8}{N}\rho\left(\frac{1-\rho^{N-1}}{1-\rho}\right)^2 \ln L}$.

Proof: At first, we consider off-diagonal elements of $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$ that can be expanded as follows:

$$\begin{aligned} \mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ij} =& \sum_{r=1}^{N}\sum_{c=1}^{N} w_{ir}\mathbf{K}_{\mathbf{x}\mathbf{x}}^{rc}w_{jc} \\ =& \sigma_X^2 \underbrace{(w_{i1}w_{j1} + \dots + w_{iN}w_{jN})}_{T_0^{ij}} \\ &+ \sigma_X^2\rho \underbrace{(w_{i1}w_{j2} + w_{i2}w_{j1} + \dots + w_{iN-1}w_{jN} + w_{iN}w_{jN-1})}_{T_1^{ij}} \\ &+ \dots + \sigma_X^2\rho^{N-1}\underbrace{(w_{i1}w_{jN} + w_{iN}w_{j1})}_{T_{N-1}^{ij}} = \sigma_X^2 \sum_{k=0}^{N-1} \rho^k T_k^{ij}. \end{aligned} \tag{4}$$

Due to symmetry of the covariance matrix, we investigate upper off-diagonal elements only, i.e., $1 \le i < j \le L$. In order to bound these elements, we evaluate an upper bound for the probability that the largest upper off-diagonal elements of $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$ is greater than $\sigma_X^2\left(\frac{1-\rho^N}{1-\rho}\right)\zeta$, where ζ is a positive real value. This probability is given by:

$$\begin{aligned} &\Pr\left\{\max_{i \ne j}|\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ij}| > \sigma_X^2\left(\frac{1-\rho^N}{1-\rho}\right)\zeta\right\} \\ &\overset{(a)}{\le} \frac{L(L-1)}{2}\Pr\left\{|\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ij}| > \sigma_X^2\left(\frac{1-\rho^N}{1-\rho}\right)\zeta\right\} \\ &= \frac{L(L-1)}{2}\Pr\left\{\frac{1}{\sigma_X^2}\left(\frac{1-\rho}{1-\rho^N}\right)|\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ij}| > \zeta\right\} \\ &\overset{(b)}{\le} L(L-1)\exp(-s\zeta)\mathbb{E}\left[\exp\left(s\frac{1}{\sigma_X^2}\left(\frac{1-\rho}{1-\rho^N}\right)\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}^{ij}\right)\right] \\ &\overset{(c)}{=} L(L-1)\exp(-s\zeta)\mathbb{E}\left[\exp\left(s\sum_{k=0}^{N-1}\kappa_k T_k^{ij}\right)\right] \end{aligned} \tag{5}$$

where (a) follows from the fact that there are only $\frac{L(L-1)}{2}$ such i.i.d. random variables [11], (b) follows form the generalized Chebyshev inequality [12] for $s \geq 0$, (c) holds form (4), and $\kappa_k = \rho^k \left(\frac{1-\rho}{1-\rho^N}\right)$ and $\sum_{k=0}^{N-1} \kappa_k = 1$. Then, we have:

$$
\begin{aligned}
&\Pr\left\{\max_{i\neq j}|\mathbf{K}^{ij}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}| > \sigma_X^2 \left(\frac{1-\rho^N}{1-\rho}\right)\zeta\right\}\\
&\overset{(a)}{\leq} L(L-1)\exp(-s\zeta)\left[\sum_{k=0}^{N-1}\kappa_k \mathbb{E}\left[\exp\left(sT_k^{ij}\right)\right]\right]\\
&\overset{(b)}{=} L(L-1)\sum_{k=0}^{N-1}\kappa_k\left[\exp(-s\zeta)\prod_{l=1}^{N_k}\mathbb{E}\left[\exp\left(sV_l^{ij}\right)\right]\right]\\
&\overset{(c)}{\leq} L(L-1)\sum_{k=0}^{N-1}\kappa_k\left[\exp(-s\zeta)\prod_{l=1}^{N_k}\exp\left(s^2\frac{\left(\frac{1}{N}-\frac{-1}{N}\right)^2}{8}\right)\right]\\
&\overset{(d)}{=} L(L-1)\sum_{k=0}^{N-1}\kappa_k\left[\exp\left(-\frac{N^2\zeta^2}{2N_k}\right)\right]\\
&= L(L-1)\left[\kappa_0\exp\left(-\frac{N\zeta^2}{2}\right)+\sum_{k=1}^{N-1}\kappa_k\exp\left(-\frac{N^2\zeta^2}{(N-k)4}\right)\right]\\
&< L(L-1)\left[\kappa_0\exp\left(-\frac{N\zeta^2}{2}\right)+\sum_{k=1}^{N-1}\kappa_k\exp\left(-\frac{N\zeta^2}{4}\right)\right]\\
&\leq L(L-1)\exp\left(-\frac{N\zeta^2}{4}\right),
\end{aligned}
\tag{6}
$$

where (a) holds due to the convexity of $\exp(\cdot)$, (b) follows from the fact that $\mathbb{E}\left[\exp(sT_k^{ij})\right]$ is the moment generating function of T_k^{ij} that is the sum of $N_k \in \{N, 2(N-1), \ldots, 2\}$ i.i.d. Bernoulli(0.5) random variables $V^{ij} = W_{ir}W_{jc} \in \{\frac{+1}{N}, \frac{-1}{N}\}$, (c) holds due to the fact that V^{ij} is a bounded random variable [13], and (d) holds by choosing $s = \frac{N^2\zeta}{N_k}$. By setting $\beta = \left(\frac{1-\rho^N}{1-\rho}\right)\zeta$, the probability can be bounded by:

$$
\Pr\left\{\max_{i\neq j}|\mathbf{K}^{ij}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}| > \sigma_X^2\beta\right\} \leq \exp\left(-\frac{N}{4}\left(\frac{1-\rho}{1-\rho^N}\right)^2\beta^2\right).
\tag{7}
$$

By substituting $\beta = \sqrt{\frac{12}{N}\left(\frac{1-\rho^N}{1-\rho}\right)^2 \ln L}$, (3a) is obtained.

For the diagonal elements of $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$ we have:

$$
\begin{aligned}
\mathbf{K}^{ii}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} &= \sigma_X^2 + \sum_{r=1}^{N}\sum_{\substack{c=1\\ r\neq c}}^{N} w_{ir}\mathbf{K}^{rc}_{\mathbf{x}\mathbf{x}}w_{ic}\\
&= \sigma_X^2 + 2\sigma_X^2\rho\underbrace{(w_{i1}w_{i2}+\cdots+w_{iN-1}w_{iN})}_{D_1^{ii}}\\
&\quad + 2\sigma_X^2\rho^2\underbrace{(w_{i1}w_{i3}+\cdots+w_{iN-2}w_{iN})}_{D_2^{ii}}\\
&\quad + \ldots + 2\sigma_X^2\rho^{N-1}\underbrace{(w_{i1}w_{iN})}_{D_{N-1}^{ii}} = \sigma_X^2 + 2\sigma_X^2\sum_{k=1}^{N-1}\rho^k D_k^{ii},
\end{aligned}
\tag{8}
$$

Similar to (5), we evaluate an upper bound for the probability that the largest deviation of diagonal elements of $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$ from σ_X^2 is greater than $2\sigma_X^2\left(\frac{\rho-\rho^N}{1-\rho}\right)\epsilon$, where ϵ is a positive real value. This probability is given by:

$$
\begin{aligned}
&\Pr\left\{\max_i|\mathbf{K}^{ii}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} - \sigma_X^2| > 2\sigma_X^2\left(\frac{\rho-\rho^N}{1-\rho}\right)\epsilon\right\}\\
&\overset{(a)}{\leq} L\Pr\left\{|\mathbf{K}^{ii}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} - \sigma_X^2| > 2\sigma_X^2\left(\frac{\rho-\rho^N}{1-\rho}\right)\epsilon\right\}\\
&\overset{(b)}{=} 2L\exp(-s\epsilon)\mathbb{E}\left[\exp\left(s\sum_{k=1}^{N-1}\lambda_k D_k^{ii}\right)\right]\\
&\overset{(c)}{\leq} 2L\exp(-s\epsilon)\left[\sum_{k=1}^{N-1}\lambda_k\mathbb{E}\left[\exp\left(sD_k^{ii}\right)\right]\right]\\
&\overset{(d)}{\leq}\sum_{k=1}^{N-1}\lambda_k\exp\left(-\frac{N^2\epsilon^2}{2(N-k)}\right) \leq \exp\left(-\frac{N\epsilon^2}{2}\right),
\end{aligned}
\tag{9}
$$

where $\lambda_k = \rho^k\left(\frac{1-\rho}{\rho-\rho^N}\right)$ and $\sum_{k=1}^{N-1}\lambda_k = 1$, (a) follows from the fact that there are only L such random variables which are identically distributed [11], (b) follows form the generalized Chebyshev inequality [12] for $s \geq 0$, (d) results from the convexity of $\exp(\cdot)$, and (e) holds following the same results of parts (c) and (d) in (6) and by choosing $s = \frac{N^2\zeta}{2(N-k)}$. By setting $\alpha = 2\left(\frac{\rho-\rho^N}{1-\rho}\right)\epsilon$, we have:

$$
\Pr\left\{\max_i|\mathbf{K}^{ij}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} - \sigma_X^2| > \sigma_X^2\alpha\right\} \leq \exp\left(-\frac{N}{8}\left(\frac{1-\rho}{\rho-\rho^N}\right)^2\alpha^2\right).
\tag{10}
$$

By substituting $\alpha = \sqrt{\frac{8}{N}\rho\left(\frac{1-\rho^{N-1}}{1-\rho}\right)^2 \ln L}$, (3b) is obtained. ■

Remark 1. For a sufficiently large N and L, $L \leq N$, $\alpha \to 0$ and $\beta \to 0$, $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$ asymptotically converges to $\sigma_X^2\mathbf{I}_L$ with high probability. Moreover, from the fact that the content source is the Gauss-Markov process, which implies that the content vector $\mathbf{x}$ is jointly Gaussian, and RP is a linear transform, the projected data $\tilde{\mathbf{x}}$ follows the jointly Gaussian distribution, i.e., $\tilde{\mathbf{X}} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}})$. Therefore, since elements of $\tilde{\mathbf{x}}$ are asymptotically uncorrelated, $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}} \approx \sigma_X^2\mathbf{I}_L$, one can conclude that $\tilde{\mathbf{x}}$ are asymptotically i.i.d. In addition, the digital fingerprint extracted from $\tilde{\mathbf{x}}$ consists of L bits that are i.i.d. Bernoulli($\frac{1}{2}$) due to symmetry of the Gaussian distribution.

B. Independent Identically Distributed Data

As mentioned in Section I, multimedia data can be modeled as i.i.d., i.e., $\mathbf{X} \sim p(\mathbf{x}) = \prod_{i=1}^{N} p(x_i)$, where $p(x_i)$ is a symmetric distribution with zero mean and the variance σ_X^2 in certain domains. For example, $p(x_i)$ can be approximated by a Generalized Gaussian distribution, due to the property of DCT or DWT coefficients of multimedia data [14], [15]. Therefore in this section we investigate the covariance matrix of projected data in order to justify the correlation induced by the RP to the i.i.d. data.

Collary 1 (*uncorrelatedness preservation property of RP*)**.** Let the elements of the RP matrix, $\mathbf{W}$, be generated as in Proposition 1, and $\mathbf{X}$ is drawn i.i.d. from a common stationary distribution with variance σ_X^2. Then, the diagonal elements of covariance matrix of the projected noise $\tilde{\mathbf{X}} = \mathbf{WX}$ are equal to σ_X^2, i.e., $\forall i, \mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}^{ii} = \sigma_X^2$, and all off-diagonal elements of $\mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}$ satisfies:

$$\Pr\left\{\max_{i \neq j} |\mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}^{ij}| > \delta\sigma_X^2\right\} < \frac{1}{L}, \qquad (11)$$

where $\delta = \sqrt{\frac{12}{N}\ln L}$.

Proof: This is a corollary of Proposition 1, where $\rho \to 0$. For the off-diagonal elements of $\mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}$, we can easily derive (11) by substituting $\rho = 0$. For the diagonal elements, $\alpha|_{\rho=0} = 0$. Thus, $\Pr\{\max_i |\mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}^{ii} - \sigma_X^2| > 0\} < \lim_{\rho \to 0} \frac{1}{L^{\left(\frac{1}{\rho}\right)}} = 0$ for all $L > 1$, which implies that $\forall i, 1 \leq i \leq L, \mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}^{ii} = \sigma_X^2$. ■

Remark 2. For a sufficiently large N and L, $L \leq N$, $\delta \to 0$ and $\mathbf{K}_{\tilde{\mathbf{X}}\tilde{\mathbf{X}}}$ converges to $\sigma_X^2 \mathbf{I}_L$ with high probability. Then, one can conclude that the samples of projected data are asymptotically uncorrelated. Moreover, in the case that the data are generated i.i.d. from the Gaussian distribution, one can conclude that the binary digital fingerprint extracted from a projected content consists of L bits that are i.i.d. Bernoulli$(\frac{1}{2})$, due to the fact that the Gaussian distribution is symmetric, and uncorrelated and identically distributed Bernoulli random variables are i.i.d.

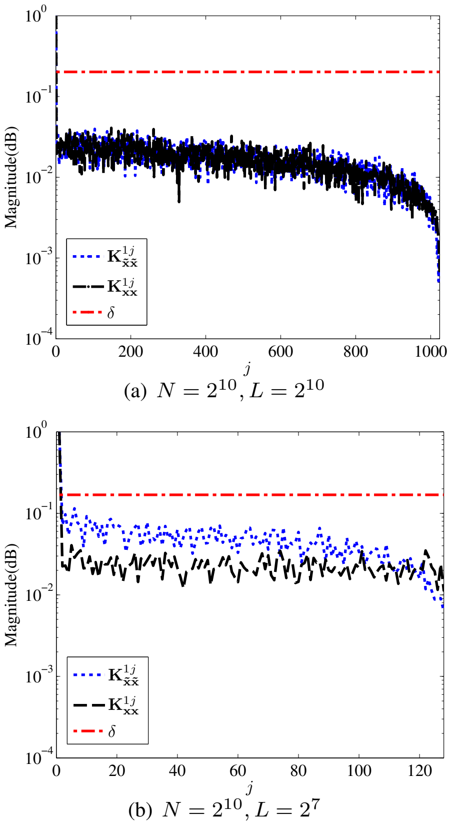
III. Simulation Results

In this Section we present experimental validation of our theoretical findings for synthetic data and real images.

First we apply the RP generated according to the setup discussed in Section II to the i.i.d. zero mean unit variance Gaussian data of length $N = 2^{10}$. Fig. 2 illustrates the impact of the RP on the the projected data with the same dimensionality (Fig. 2(a)) and the reduced dimensionality (Fig. 2(b)). It is possible to observe that such a transform nearly preserves the uncorrelatedness of its i.i.d. input according to the upper bound (11) defined in Proposition 1.

The second set of tests was dedicated to the experimental justification of the decorrelation capabilities of the RP. For this purpose, we carried out a number of experiments, where the input data are generated from a Gauss-Markov process with the normalized correlation coefficient $0.5 \leq \rho \leq 0.95$. The results are demonstrated only for $\rho = 0.95$ and 0.75 (Fig. 3). These results confirm the theoretical finding of Proposition 1 stating that the residual correlation is accurately upper bounded by (3a).

The third set of tests is assigned to the RP uncorrelatedness preservation and decorrelation capabilities for real images in DCT and spatial domains. The tests have been performed for a set of 1180 images of African animals with size 256×384 from Corel image collection provided by Duygulu *et al.* [16]. Fig. 4 illustrates the RP application to the real images in different domains. The results presented in Fig. 5(a) and Fig. 6(a) demonstrate the average two dimensional autocorrelation for 1180 real images in DCT and spatial domains, the last 512 elements of the average autocorrelation of projected DCT coefficients (Fig. 5(b)) and real images (Fig. 6(b)) using RP, and finally the last 512 elements of the average autocorrelation of the extracted digital fingerprints (Fig. 5(c) and Fig. 6(c)). The obtained results demonstrate that elements of extracted binary fingerprints are almost uncorrelated.



(a) $N = 2^{10}, L = 2^{10}$

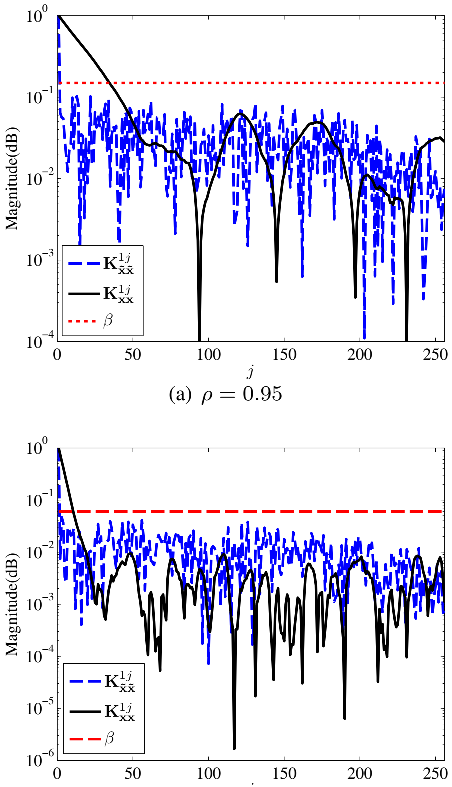
(b) $N = 2^{10}, L = 2^7$

Fig. 2. I.i.d. preservation property of RP: (a) the first row of $\mathbf{K}_{\mathbf{xx}}$ and $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$, and (b) the first 128 elements of the first row of $\mathbf{K}_{\mathbf{xx}}$ and $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$. $\mathbf{x}$ is generated from the i.i.d. Gaussian process with $\sigma_X^2 = 1$. δ represents the upper bound on the maximum value of non-diagonal elements of $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$.

The obtained results justify the accuracy of Proposition 1 applied to real data in the coordinate and DCT transform domains. Furthermore, the results from Fig. 5 and Fig. 6 indicate that the correlation between the samples of the digital fingerprints extracted from images in DCT and spatial domain are approximately the same under the explained RP. Consequently, one can conclude that by directly using RP in spatial domain instead of joint usage of the DCT and RP, the digital fingerprints with the same properties can be extracted with a lower complexity.

IV. Conclusions

In this paper, we presented a statistical analysis of digital fingerprint extraction using the RP. We succeeded to demonstrate that the output of the RP for this type of input has an asymptotically diagonal covariance matrix with high probability.



(a) $\rho = 0.95$

(b) $\rho = 0.75$

Fig. 3. The first 256 elements of the first row of $\mathbf{K}_{\mathbf{xx}}$ and $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$, where $\mathbf{x}$ is generated from the Gauss-Markov process with $\sigma_X^2 = 1$. $\mathbf{x}$ and $\tilde{\mathbf{x}}$ have the length of $N = 2^{15}$ and $L = 2^8$, respectively. δ represents the upper bound on the maximum value of non-diagonal elements of $\mathbf{K}_{\tilde{\mathbf{x}}\tilde{\mathbf{x}}}$.

Since the RP are only approximate orthoprojectors, we analyzed the correlation that such a transform might induce into i.i.d. models of images in some domains like DCT and DWT. Using a similar statistical arguments we showed that the data in the RP domain will converge to a diagonal covariance matrix with high probability. Our theoretical findings were successfully confirmed by a set of experimental results for synthetic data and real images.

Acknowledgment

The authors would like to thank M. Meckes and V. Balakirsky for the stimulating discussions. This paper was partially supported by SNF projects 200020-134595.

References

[1] 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.

[2] J. Fridrich, "Robust bit extraction from images," in *Proc. of MCS*, vol. 2, july 1999, pp. 536 –540.

[3] J. Haitsma and T. Kalker, "A highly robust audio fingerprinting system." in *International Conference Music Information Retrieval*, 2002.

[4] A. K. Jain, *Fundamentals of digital image processing*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1989.

[5] G. Golub and C. van Loan, *Matrix Computations*. Oxford, UK: North Oxford Academi, 1983.

[6] S. Voloshynovskiy, O. Koval, F. Beekhof, F. Farhadzadeh, and T. Holotyak, "Information-theoretical analysis of private content identification," in *Proc. of ITW*, Dublin, Ireland, 2010.

[7] M. A. Davenport, P. T. Boufounos, M. B. Wakin, and R. G. Baraniuk, "Signal processing with compressive measurements," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 445–460, 2010.

[8] W. B. Johnson and J. Lindenstrauss, "Extensions of lipschitz mapping into hilbert space," in *Conf. in MAP*, ser. Contemporary Mathematics, vol. 26. AMS, 1984, pp. 189–206.

[9] O. Koval and S. Voloshynovskiy, "Multimodal object authentication with random projections: a worst-case approach," in *Proceedings of SPIE / Media Forensics and Security XII*, San Jose, USA, January 21–24 2010.

[10] A. L. Varna, A. Swaminathan, and M. Wu, "A decision theoretic framework for analyzing hash-based content identification systems," in *ACM Digital Rights Management Workshop*, October 2008, pp. 67–76.

[11] G. Caraux and O. Gascuel, "Bounds on distribution functions of order statistics for dependent variates," *Statistics & Probability Letters*, vol. 14, no. 2, pp. 103 – 105, 1992.

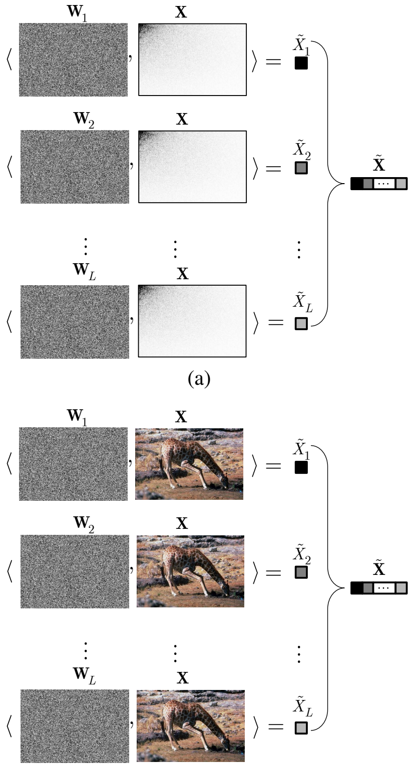
[12] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: John Wiley & sons, 1968.

[13] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[14] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, pp. 674–693, 1989.

[15] S. LoPresto, K. Ramchandran, and M. Orchard, "Image coding based on mixture modeling of wavelet coefficients and a fast estimation-quantization framework," in *Proc. of Conf. on Data Compression*. Washington, DC, USA: IEEE Computer Society, 1997.

[16] P. Duygulu, K. Barnard, J. F. G. d. Freitas, and D. A. Forsyth, "Object recognition as machine translation: Learning a lexicon for a fixed image vocabulary," in *Proceedings of the 7th European Conference on Computer Vision-Part IV*, ser. ECCV '02, 2002, pp. 97–112.



(a)

(b)

Fig. 4. Two dimensional data projection by the RP: (a) DCT domain, and (b) spatial domain.

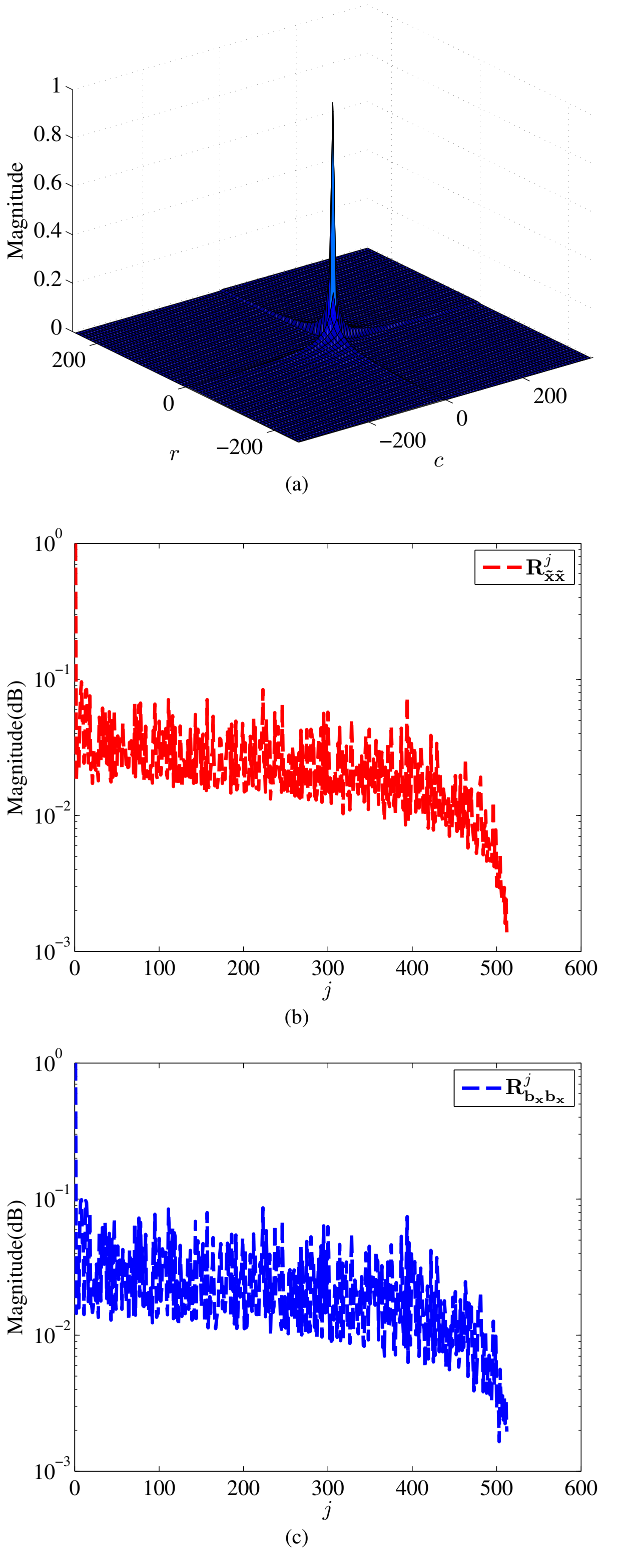


Fig. 5. I.i.d. preservation property of RP for real images: (a) the average two dimensional autocorrelation of the 2D-DCT of real images, (b) the last 512 elements of the average autocorrelation of projected DCT coefficients using RP, and (c) the last 512 elements of the average autocorrelation of the extracted digital fingerprints. $\mathbf{R}^j_{\mathbf{xx}}$ and $\mathbf{R}^j_{\mathbf{b_x b_x}}$ denote the j^{th} element of autocerrelation of a projected data and an extracted digital fingerprint, respectively.

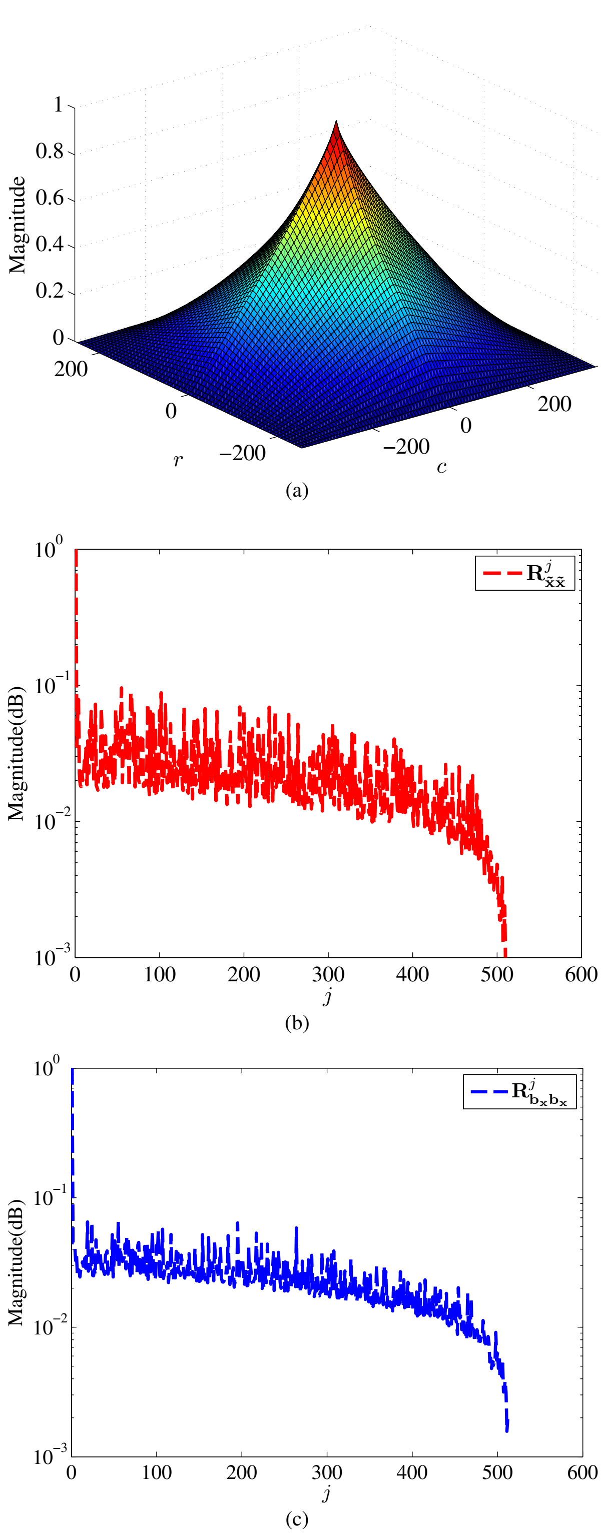


Fig. 6. Decorrelation property of RP for real images: (a) the average two dimensional autocorrelation of the set of real images, (b) the last 512 elements of the average autocorrelation of projected images using RP, and (c) the last 512 elements of the average autocorrelation of the extracted digital fingerprints. $\mathbf{R}^j_{\mathbf{xx}}$ and $\mathbf{R}^j_{\mathbf{b_x b_x}}$ denote the j^{th} element of autocerrelation of a projected data and an extracted digital fingerprint, respectively.