SCALE-ROBUST COMPRESSIVE CAMERA FINGERPRINT MATCHING WITH RANDOM PROJECTIONS

Diego Valsesia, Giulio Coluccia, Tiziano Bianchi, Enrico Magli

Dipartimento di Elettronica e Telecomunicazioni – Politecnico di Torino, Italy

ABSTRACT

Recently, we demonstrated that random projections can provide an extremely compact representation of a camera fingerprint without significantly affecting the matching performance. In this paper, we propose a new construction that makes random projections of camera fingerprints scale-robust. The proposed method maps the compressed fingerprint of a rescaled image to the compressed fingerprint of the original image, rescaled by the same factor. In this way, fingerprints obtained from rescaled images can be directly matched in the compressed domain, which is much more efficient than existing scale-robust approaches. Experimental results on the publicly available Dresden database show that the proposed technique is robust to a wide range of scale transformations. Moreover, robustness can be further improved by providing reference scales in the database, with a small additional storage cost.

***Index Terms*—** PRNU, random projections

1. INTRODUCTION

Many important forensics tasks, including device identification, device linking, recovery of processing history, detection of digital forgeries, can be performed by relying on specific sensor fingerprints that link each image to a particular acquisition device. In this sense, the photo-response nonuniformity (PRNU) of digital imaging sensor [1], which is due to slight variations in the properties of individual pixels, is a widely used fingerprint, since it provides robustness to common operations like lossy compression and image resizing [2, 3].

Despite its good camera identification performance, practical use of PRNU as a sensor fingerprint must face two important problems. The first one is that the PRNU pattern has the same size as the imaging sensor, which typically counts tens of millions of pixels. As a consequence, a realistic database of a few thousand sensor fingerprints would require to store more than 10^{10} individual pixel values in uncompressed format. The second problem is that the test image should be geometrically aligned with the fingerprint in the database. Since many images are routinely resized and/or cropped, *e.g.*, when they are posted on specific photo sharing services, the required synchronization step can make camera identification a very time consuming procedure.

As to the management of a large database of PRNU camera fingerprints, several solutions have been proposed in the literature. In [4, 5], the authors introduced a so-called *fingerprint digest* obtained by keeping only a fixed number of the largest fingerprint values and their positions, which enables a fast search strategy with constant size fingerprints [6]. In [7], the authors proposed to represent sensor fingerprints in binary-quantized form: even though the size of binary fingerprints scales with sensor resolution, binarization can considerably speed-up the fingerprint matching process.

Recently, in [8] we proposed a compact representation of PRNU fingerprints based on a fixed number of random projections. Thanks to the Johnson-Lindenstrauss (JL) lemma [9], the proposed representation achieves camera identification performance very close to uncompressed PRNU fingerprints. Moreover, random projections can be optionally binary-quantized, leading to an extremely compact fingerprint representation. Results indicated that the proposed compressed fingerprints sensibly outperform both fingerprint digests and standard binary fingerprints with the same length.

Concerning the synchronization problem, existing approaches are based either on a generalized likelihood ratio test (GLRT) approach [10], through a brute force search of possible scale and/or crop parameters, or on defining the fingerprint detector in a transform invariant domain [11]. However, the first strategy usually requires an expensive search, while the second approach can only by applied to a specific geometrical transformation. Even if fingerprint digests can be used to speed up the GLRT approach [12], their complexity is still too high in the case of very large databases.

In this paper, we propose to extend the random projection technique by employing a specific construction of the projection matrix that is robust to image resizing. Namely, the new compressed fingerprint has the property that a rescaled version of the image corresponds to a rescaled version of the fingerprint. In this way, fingerprint synchronization can be performed directly in the compressed domain, leading to a much more efficient matching process with respect to existing approaches. The robustness of the method to different scale factors can be further improved by providing in the database

This work is supported by the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013) / ERC Grant agreement n.279848.

a certain number of anchor points obtained by computing differently rescaled version of the fingerprint for a fixed set of scale factors.

2. COMPRESSIVE PRNU FORENSICS

PRNU [1, 13] of imaging sensors is a property unique to each sensor array due to impurities in silicon wafers and its effect is a noise pattern affecting every image taken by that specific sensor. Hence, the PRNU can be thought of as a *fingerprint* of the sensor used to take a specific picture or a set of pictures. The PRNU has the same pixel size as the sensor, and every optical sensor exhibits PRNU. It is stable under different environmental conditions and is robust to several signal processing operations. The PRNU characterizing one sensor can be extracted from a set of (not completely dark) pictures taken by the same camera (20 to 50), with the procedure detailed in the references above. Its knowledge can solve a set of problems, like $i)$ The *device identification* problem [2], testing whether a given picture was taken by a specific device; $ii)$ the *device linking* problem [14], presented with two images and determining whether they have been acquired by the same device.; $iii)$ the *fingerprint matching* problem, whose goal is determining which device in a database (if present) has acquired a given set of pictures taken by the same camera.

Due to its noise-like characteristic, PRNU cannot be easily compressed. Hence, a database containing a significant number of length-n PRNU fingerprints, n being the pixel-size of the optical sensor, can rapidly grow in size. For this reason, in [8] we proposed a method to "compress" this database with negligible information loss using Random Projections (RP), exploiting the low correlation between different PRNUs. The idea, based on the key property of the Johnson–Lindenstrauss lemma [9], was to project the original n–dimensional data to a m–dimensional subspace, with $m < n$, using a random matrix $\mathbf{\Phi} \in \mathbb{R}^{m \times n}$. Hence, a collection of N n–dimensional fingerprints of known cameras, $\mathbf{D} \in \mathbb{R}^{n \times N}$, is reduced to a m–dimensional subspace $\mathbf{A} \in \mathbb{R}^{m \times N}$ by

$$\mathbf{A} = \mathbf{\Phi}\mathbf{D} \,. \tag{1}$$

For what concerns the *fingerprint matching* problem (and the conceptually very similar problem of *camera identification*), a test fingerprint (or its counterpart in the camera identification problem) $\hat{\mathbf{k}} \in \mathbb{R}^n$ is first compressed using the same $\mathbf{\Phi}$ used to compress the database, namely

$$\mathbf{y} = \mathbf{\Phi}\hat{\mathbf{k}} \,, \tag{2}$$

then compared to each column of the compressed database $\mathbf{A}$ to find the most correlated. Refer to [8] for further details.

Several technical issues may arise in this framework. The first problem is the complexity related to the generation and storage of a fully random sensing matrix. The second is the complexity related to the matrix-matrix product of (1). Both issues can be mitigated by using a partial circulant sensing matrix, which allows to generate of a lower number of random coefficients and to efficiently perform the product using the FFT, maintaining the distance-preserving properties in the compressed domain [15, 16].

Finally, further compression can be obtained with binary quantization of the compressed database, *i.e.*, reducing the compressed database to the matrix of its signs only,

$$\mathbf{A} = \mathrm{sign}(\mathbf{\Phi}\mathbf{D}) \qquad \mathbf{y} = \mathrm{sign}(\mathbf{\Phi}\hat{\mathbf{k}}). \tag{3}$$

In the case of binary measurements the correlation coefficient is replaced by the Hamming distance as test metric.

3. SCALE–ROBUST RANDOM PROJECTIONS

A compressive camera identification system typically has to deal with unknown image transformations of the query image. In this section, we propose a method to cope with rescaled images. Existing solutions typically rely on maximizing the the GLRT with respect to the transformation parameter (*i.e.,* the scale in this case) [10]. This solution requires an expensive search to determine the scaling factor because a cross-correlation function has to be computed from high-dimensional fingerprints. Alternative solutions, like the creation of a fingerprint digest [12], where only the d largest components of the fingerprint and their relative positions are stored, can be used to alleviate the computational burden. However, even if this solution is competitive in terms of computational complexity of the matching operation from scaled pictures, it is not also good for compression as it was shown to be outperformed by random projections [8]. We thus seek solutions to make random projections robust to scale transformations, so that when presented a scaled photo, the system can correctly identify the imaging sensor that acquired it by only keeping a database of random projections of PRNU patterns and the information on the original sensor size and computing random projections of the query pattern.

The ability to correctly match a rescaled query image with the corresponding entry in the compressed database requires a compression operation that ideally maps the compressed fingerprint of the rescaled image to the compressed fingerprint of the original image, rescaled by the same factor. To achieve this goal, we propose a novel construction for the sensing matrix, based on block circulant with circulant blocks (BCCB) matrices, and a new matching process entirely in the compressed domain.

3.1. Construction of the sensing matrix

While [8] investigated the use of circulant matrices thanks to the fast implementation allowed by such operator and the significant body of theoretical work around them, this work uses BCCB matrices as sensing matrices $\mathbf{\Phi}$ in the products (1) and (2). The performance of random BCCB matrices was studied in [17, 18] where they were shown to satisfy the Restricted Isometry Property (RIP) [19]. The RIP is concerned with embeddings of sparse signals, while here we seek an embedding satisfying the Johnson–Lindenstrauss lemma (JL) [9]. However, Krahmer and Ward [20] showed that randomizing the

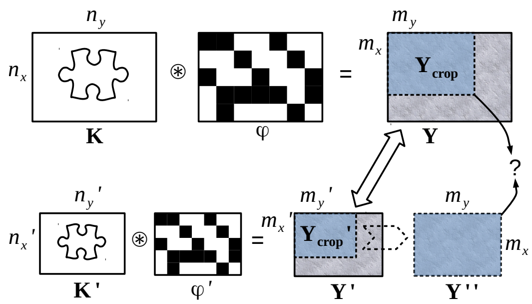


Fig. 1: Block diagram of the proposed technique. Above: creation of an entry in the database. Below: matching technique.

column signs of a matrix satifying the RIP, provides a JL embedding, satisfying our goal. We remark that we are interested in a very particular class of signals, PRNU patterns, which can be modeled as white Gaussian noise. Randomizing the column signs of the sensing operator amounts to randomizing the signs of the signal and using the original operator. However, since our signals of interest are made of white Gaussian noise, the randomization of the signs has no effect and it is possible to omit it.

BCCB operators can be efficiently implemented via the two-dimensional discrete Fourier transform. In practice, we move from considering vectorized versions of the fingerprint to be compressed to a two dimensional representation, since

$$\mathbf{\Phi} \cdot \mathrm{vec}\{\mathbf{X}\} = \mathrm{vec}\{\boldsymbol{\varphi} \circledast \mathbf{X}\} \ ,$$

where $\boldsymbol{\varphi}$ is a random matrix (i.i.d. Gaussian) of the same size of $\mathbf{X}$ such that $\mathrm{vec}\{\boldsymbol{\varphi}\}$ is the first row of the BCCB sensing matrix $\mathbf{\Phi}$, and $\circledast$ is the two-dimensional circular convolution, which can be efficiently implemented as

$$\boldsymbol{\varphi} \circledast \mathbf{X} = \mathrm{IDFT}_2[\mathrm{DFT}_2[\mathbf{X}] \cdot \mathrm{DFT}_2[\boldsymbol{\varphi}]] \ . \qquad (4)$$

Hence, the scale-robust system will create the random matrix $\boldsymbol{\varphi}_{\max}$ of size $n_x^{\max} \times n_y^{\max}$, where the size coincides with the maximum sensor size the system deals with.

3.2. Creation of an entry in the database

Referring to the above part of Fig. 1, the procedure to create a compressed database entry is the following. Given a fingerprint $\mathbf{K}$ of size $n_x \times n_y$, first $\boldsymbol{\varphi}_{\max}$ is resized to match the size of $\mathbf{K}$, to obtain $\boldsymbol{\varphi}$. Then, the convolution between $\mathbf{K}$ and $\boldsymbol{\varphi}$ is efficiently performed using (4), obtaining $\mathbf{Y}$. Finally, to effectively obtain dimensionality reduction, a contiguous area of $\mathbf{Y}$ of size $m_x \times m_y$ is cropped, obtaining $\mathbf{Y}_{\mathrm{crop}}$, which is then stored as an entry of the database. A way to crop the same area from an arbitrarly resized version of $\mathbf{Y}$ (*e.g.*, always crop the top-left corner and store the ratios $\frac{m_x}{n_x}$ and $\frac{m_y}{n_y}$) is stored, as well. The algorithm is reported in Alg. 1.

In case of binary measurements, the database stores the 1-bit quantized version of $\mathbf{Y}$.

3.3. Matching

As for the matching operations, we refer to the bottom part of Fig. 1. The matching between a test fingerprint $\mathbf{K}'$ of a

Algorithm 1 Creation of an entry in the database

Require: A fingerprint $\mathbf{K}$ of size $n_x \times n_y$, $\boldsymbol{\varphi}_{\max}$
 $\boldsymbol{\varphi} \leftarrow$ resize of $\boldsymbol{\varphi}_{\max}$ to size $n_x \times n_y$
 $\mathbf{Y} \leftarrow \mathrm{IDFT}_2[\mathrm{DFT}_2[\mathbf{K}] \cdot \mathrm{DFT}_2[\boldsymbol{\varphi}]]$
 $\mathbf{Y}_{\mathrm{crop}} \leftarrow$ top-left crop from $\mathbf{Y}$ of size $m_x \times m_y$
 Store $\mathbf{Y}_{\mathrm{crop}}$ in database $\mathbf{A}$: $\mathbf{A}^i = \mathbf{Y}_{\mathrm{crop}}$
 Store $\frac{m_x}{n_x}$ and $\frac{m_y}{n_y}$

rescaled image and the i-th entry in the database $\mathbf{A}^i$ is performed as follows. Given a fingerprint $\mathbf{K}'$ of size $n'_x \times n'_y$, first $\boldsymbol{\varphi}_{\max}$ is resized to match the size of $\mathbf{K}'$, to obtain $\boldsymbol{\varphi}'$. Then, the convolution between $\mathbf{K}'$ and $\boldsymbol{\varphi}'$ is efficiently performed using (4), obtaining $\mathbf{Y}'$. $\mathbf{Y}'$ is then cropped to the same contiguous area of $\mathbf{A}^i$ as in the database (e.g., if it was top-left, then crop the top-left $\frac{m_x}{n_x} n'_x \times \frac{m_y}{n_y} n'_y$ pixels), obtaining $\mathbf{Y}'_{\mathrm{crop}}$. Finally, $\mathbf{Y}'_{\mathrm{crop}}$ is resized to $m_x \times m_y$, obtaining $\mathbf{Y}''$. Hence, $\mathbf{Y}''$ is synchronized with $\mathbf{A}^i$, making the correlation evaluation possible. The entire process is summarized in Alg. 2. Note that the resizing of the cropped random projections of the test fingerprint must be repeated for every entry of the database because of the different values of $\frac{m_x}{n_x}$ and $\frac{m_y}{n_y}$. In

Algorithm 2 Scale-robust matching process

Require: A test fingerprint $\mathbf{K}'$ of size $n'_x \times n'_y$, $\boldsymbol{\varphi}_{\max}$, the database $\mathbf{A}$
 for all entries in the database $\mathbf{A}$ **do**
  $\boldsymbol{\varphi}' \leftarrow$ resize of $\boldsymbol{\varphi}_{\max}$ to size $n'_x \times n'_y$
  $\mathbf{Y}' \leftarrow \mathrm{IDFT}_2[\mathrm{DFT}_2[\mathbf{K}'] \cdot \mathrm{DFT}_2[\boldsymbol{\varphi}']]$
  $\mathbf{Y}'_{\mathrm{crop}} \leftarrow$ top-left crop from $\mathbf{Y}'$ of size $\frac{m_x}{n_x} n'_x \times \frac{m_y}{n_y} n'_y$
  $\mathbf{Y}'' \leftarrow$ resize of $\mathbf{Y}'_{\mathrm{crop}}$ to size $m_x \times m_y$
  $\rho_i \leftarrow \mathrm{corr}(\mathbf{Y}'', \mathbf{A}^i)$
 end for
Ensure: $i = \arg\max_i \rho_i$

case of binary measurements, the cropped test measurement is first resized and then its sign is kept. Finally, Hamming distance is used as dissimilarity metric.

We remark here that the matching process could be also performed by resizing the test fingerprint of a rescaled image to the size of the entry stored in the database (the original $n_x \times n_y$). Nevertheless, this would require to perform the subsequent operations in the image size domain rather than in the compressed domain, with larger sizes and hence additional complexity. Moreover, we tested (but omit the corresponding results for brevity) the performance of the scheme of [8] applied to a rescaled test image interpolated to the original size, proving that it is lower than the scheme proposed here.

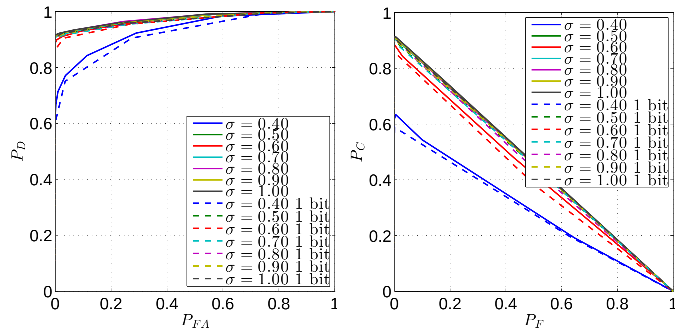
3.4. Redundant Dictionaries

The work in [8] and the previous section consider the creation of a database of compressed fingerprints where each camera sensor is associated to a single entry. An extension of this concept is possible by associating multiple entries to the same camera sensor in order to improve the robustness of the system to transformations (and, more specifically, to scaling). We call this construction of the database a redundant database. This represents a trade-off between storage and resilience to transformations, since experiments show that robust performance is observed locally around a reference scale.

It is observed that the technique proposed in section 3 best performs for detection of small scaling factors due to the interpolation processes occurring at various stages. It is thus advisable to introduce some redundancy in the database of compressed fingerprints in the form of compressed versions of fingerprints at various scales. Such redundant elements will serve as reference scales, ideally providing a closer match to the unknown scale of the fingerprint under test.

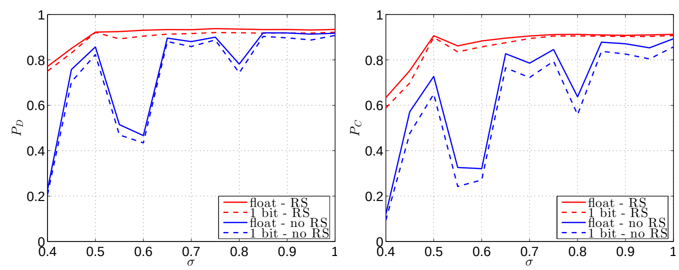
4. NUMERICAL RESULTS

We tested the method presented in Section 3 to provide robustness to scale transformations with and without reference scales in a redundant database assembled from the publicly available Dresden image database [21]. We used the flatfield images to extract the database fingerprints and the natural images for testing. The results show that the method works both for floating point measurements and binary measurements. As expected a degradation of the performance is observed as the scaling factor σ (σ^2 is the ratio of the number of pixels in the resized image to original number of pixels) decreases. This effect can be mitigated by introducing some reference scales in the database. Surprisingly, it is observed that introducing a reference scale σ_{ref} boosts the detection performance even for higher scales, *i.e.* $\sigma > \sigma_{\text{ref}}$, and not only lower scales. We refer to the metrics defined in [8] for performance assessment, *i.e.* probability of correct/wrong fingerprint to be above a threshold (P_D,P_{FA}), and probability of only/not only the correct fingerprint to be above threshold (P_C,P_F). All the tests used $m_x = 715$, $m_y = 715$. Observing Fig. 2, it can be noticed that the system performs close to the one in [8, Fig. 3] thanks to including reference scales $\sigma = 0.8, 0.55$ in addition to $\sigma = 1$. Notic The relative performance of binary measurements with respect to floating point measurements is aligned with what observed in [8]. Fig. 3 shows the maximum detection (correct detection) rates for a fixed false alarm (false detection) rate, as function of the scale. This highlights the robustness of the system to a wide range of scale transformations, especially in presence of a moderately redundant database (bottom curves represent the system without additional reference scales). As a final remark, all the tests used bicubic interpolation for all rescaling operations, including the creation of scaled versions of the test images of the Dresden database. It was noticed that bilinear interpolation works equally well. A mismatch between the two methods (*e.g.* photos scaled using bilinear interpolation and measurements scaled with bicubic) does not change the performance. However, it was observed that nearest neighbor interpolation of the measurements does not provide satisfactory results.



(a) True Positive vs. False Positive rates (b) True Detection vs. False Acceptance rates

Fig. 2: ROC curves for the Dresden database at various scales σ. $m = 715^2$ floating point/binary measurements. With reference scales.



(a) True Positive rate for $P_{FA} < 0.1$ (b) True Detection rate for $P_F < 0.1$

Fig. 3: True Positive and True Detection rates for the Dresden database at various scales σ. $m = 715^2 \simeq 512{,}000$ floating point/binary measurements. With and without reference scales (RS).

5. CONCLUSIONS AND FUTURE WORK

In this paper, we showed how the compression of camera fingerprints with random projections, originally introduced in [8], can be extended to deal with images subject to an arbitrary scaling. This is a relevant issue in real applications since photos are often resized either manually by users or automatically by photo-sharing websites. The proposed technique allows to perform all operations in the compressed domain, thanks to a novel construction of the sensing matrix. The resulting system displays excellent resilience to a wide range of scale transformations and can be further improved by including reference scales in the database of fingerprints, thus trading off storage and resilience. Finally, we remark that BCCB sensing matrices open the way to novel compressed-domain applications, thanks to the ability to directly map 2D signal processing operations to the domain of random projections as explained in [22]. Thus, future work will focus on the use of such techniques to deal with cropped images and other detection metrics like the Peak-to-Correlation Energy (PCE).

6. REFERENCES

[1] J. Lukáš, J. Fridrich, and M. Goljan, "Determining digital image origin using sensor imperfections," in *Proc. SPIE Electronic Imaging, Image and Video Communication and Processing*, 2005, vol. 5685, pp. 249–260.

[2] J. Lukáš, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 2, pp. 205–214, June 2006.

[3] Mo Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 1, pp. 74–90, March 2008.

[4] M. Goljan, J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," in *Proc. SPIE, Media Forensics and Security II*, 2010, vol. 7541, pp. 754108–754108–12.

[5] Y. Hu, B. Yu, and C. Jian, "Source camera identification using large components of sensor pattern noise," in *Computer Science and its Applications, 2009. CSA '09. 2nd International Conference on*, Dec 2009, pp. 1–5.

[6] Y. Hu, C. Li, Z. Lai, and S. Zhang, "Fast camera fingerprint search algorithm for source camera identification," in *Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on*, May 2012, pp. 1–5.

[7] S. Bayram, H.T. Sencar, and N. Memon, "Efficient sensor fingerprint matching through fingerprint binarization," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 4, pp. 1404–1413, 2012.

[8] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, "Compressed fingerprint matching and camera identification via random projections," Submitted, 2014.

[9] W.B. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," *Contemporary Mathematics*, vol. 26, 1984.

[10] M. Goljan and J. Fridrich, "Camera identification from cropped and scaled images," in *Proc. SPIE, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 2008, vol. 6819, pp. 68190E–68190E–13.

[11] D.-K. Hyun, S.-J. Ryu, M.-J. Lee, J.-H. Lee, H.-Y. Lee, and H.-K. Lee, "Source camcorder identification from cropped and scaled videos," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, 2012, pp. 83030E–83030E.

[12] M. Goljan and J. Fridrich, "Sensor fingerprint digests for fast camera identification from geometrically distorted images," in *Proc. SPIE, Media Watermarking, Security, and Forensics 2013*, 2013, vol. 8665, pp. 86650B–86650B–10.

[13] J. Fridrich, "Digital image forensics," *Signal Processing Magazine, IEEE*, vol. 26, no. 2, pp. 26–37, 2009.

[14] M. Goljan, Mo Chen, and J. Fridrich, "Identifying common source digital camera from image pairs," in *Image Processing, 2007. ICIP 2007. IEEE International Conference on*, Sept 2007, vol. 6, pp. VI – 125–VI – 128.

[15] A. Hinrichs and J. Vybíral, "Johnson-Lindenstrauss Lemma for Circulant Matrices," *Random Struct. Algorithms*, vol. 39, no. 3, pp. 391–398, Oct. 2011.

[16] H. Rauhut, "Circulant and Toeplitz Matrices in Compressed Sensing," in *SPARS'09 - Signal Processing with Adaptive Sparse Structured Representations*, 2009.

[17] F. Sebert, Y.M. Zou, and L. Ying, "Toeplitz block matrices in compressed sensing and their applications in imaging," in *Information Technology and Applications in Biomedicine, 2008. ITAB 2008. International Conference on*, May 2008, pp. 47–50.

[18] F. Sebert, L. Ying, and Y.M. Zou, "Toeplitz block matrices in compressed sensing," *CoRR*, vol. abs/0803.0755, 2008.

[19] E.J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comptes Rendus Mathematique*, vol. 346, no. 9, pp. 589–592, 2008.

[20] F. Krahmer and R. Ward, "New and Improved Johnson–Lindenstrauss Embeddings via the Restricted Isometry Property," *SIAM Journal on Mathematical Analysis*, vol. 43, no. 3, pp. 1269–1281, 2011.

[21] T. Gloe and R. Böhme, "The Dresden Image Database for benchmarking digital image forensics," *Journal of Digital Forensic Practice*, vol. 3, no. 2-4, pp. 150–159, 2010.

[22] D. Valsesia and E. Magli, "Compressive signal processing with circulant sensing matrices," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, May 2014, pp. 1015–1019.