A COMPRESSIBLE TEMPLATE PROTECTION SCHEME FOR FACE RECOGNITION BASED ON SPARSE REPRESENTATION

Yuichi Muraki[*], *Masakazu Furukawa*[*], *Masaaki Fujiyoshi*[*], *Yoshihide Tonomura*[†], *and Hitoshi Kiya*[*]

[*] Department of Information and Communication Systems, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan
[†] NTT Network Innovation Laboratories, Japan

ABSTRACT

In applications using face recognition, facial images called templates should be securely managed for privacy protection and security. This paper studies a sparse representation-based face recognition system with a new template protection scheme. The proposed scheme uses two transformations for template protection; random pixel permutation and downsampling. Thanks to these transformations, protected templates can be efficiently compressed, whereas conventional schemes do not offer such functionality. Experimental results demonstrate that the system does not degrade face recognition performance even facial templates are protected. Thus, the proposed scheme can reduce the size of the template repository in practical face recognition systems.

Index Terms— Cancelable Biometrics, Authentication, Random Projection, Noise Addition, Compressed Sensing

1. INTRODUCTION

Face recognition is useful for many applications such as personal authentication and video surveillance systems. To improve recognition performance, various methods have been studied such as eigenfaces [1], fisherfaces [2], laplacianfaces [3], and so on. Recently, a robust method based on sparse representation [4] has drawn a lot of attention in terms of recognition performance. These methods, however, have a problem; Facial images are not protected, i.e., users' privacy will not be protected when facial images are leaked, whereas secure data management is essential [5–10].

To protect original biometric templates such as iris, fingerprint, and facial images, cancelable biometrics-based authentication systems have been proposed [11]. In these systems, original templates are severely distorted by a series of intentional transformations to be protected, whereas biometric cryptosystems [12] use data hiding and/or encryption. Even so, templates can be compared in the distorted domain because all templates including a query image are transformed in the same way.

The concept of cancelable biometrics has been introduced to sparse representation-based classification. For iris recognition, a secure method based on sparse representation has been proposed [13] where a dimension reduction technique called random projection (RP) is used as the template protection scheme, similarly to many previous works [14–16]. Another template protection scheme has been proposed [17] for the sparse representation-based face recognition system [4], where this scheme adds a noise image to all facial images and clips the pixel values of noise-added images. By these schemes, templates become random noise images, so it is hard to compress protected templates efficiently. That is, the size of the storage for keeping templates linearly increases in direct proportion to the number of templates. In addition, many of these systems require the protection key which is used for face image registration when face recognition is carried out. So the key must be also managed securely.

This paper proposes a new template protection scheme for sparse presentation-based face recognition system. The proposed scheme consists of random pixel permutation and downsampling. The combination of two transformations achieves two benefits; 1) it is difficult to estimate original templates from protected templates, even if protection keys are disclosed, and 2) data size of protected templates can be reduced efficiently by lossless compression. Furthermore, there is no need of protection key management because this system can disclose the key thanks of benefit 1). Experimental results using multiple facial databases demonstrate that the proposed face recognition system with the scheme does not degrade the recognition performance even facial templates are non-invertibly protected and that the performance is comparable with the conventional scheme [13].

2. PRELIMINARIES

This section introduces the sparse representation-based face recognition [4] and the requirements for template protection schemes.

2.1. Sparse Representation-Based Face Recognition

Training image $\mathbf{I}_{i,n_i} \in \mathbb{R}^{H\times W}$ which is the n_i-th image for the i-th person is vectorized to feature vector $\mathbf{v}_{i,n_i} \in \mathbb{R}^M$, where M is often equal to HW and $n_i = 1,2,\ldots,N_i$. For the i-th registered person among K registered persons where $i = 1,2,\ldots,K$, set of N_i training vectors

$$\mathbf{A}_i = [\mathbf{v}_{i,1},\ldots,\mathbf{v}_{i,N_i}] \tag{1}$$

are given ahead. In this method [4], it is assumed that $\mathbf{y} \in \mathbb{R}^M$, the feature vector of query image $\mathbf{I}_q \in \mathbb{R}^{H\times W}$ which belongs

to the i-th person, is linearly approximated solely by the training vectors of the i-th person:

$$\mathbf{y} = \mathbf{v}_{i,1}x_{i,1} + \cdots + \mathbf{v}_{i,N_i}x_{i,N_i} = \mathbf{A}_i\mathbf{x}_i. \tag{2}$$

Therefore, with all training vectors of K registered persons, $\mathbf{y}$ can be represented as

$$\mathbf{y} = \mathbf{A}_1\mathbf{0} + \cdots + \mathbf{A}_{i-1}\mathbf{0} + \mathbf{A}_i\mathbf{x}_i + \mathbf{A}_{i+1}\mathbf{0} + \cdots + \mathbf{A}_K\mathbf{0} = \mathbf{A}\mathbf{x}_0, \tag{3}$$

where

$$\mathbf{A} = [\mathbf{A}_1 \ldots \mathbf{A}_K] \in \mathbb{R}^{M\times N}, \tag{4}$$

$$\mathbf{x}_0 = [\mathbf{0}, \ldots, \mathbf{0}, \mathbf{x}_i, \mathbf{0}, \ldots, \mathbf{0}] \in \mathbb{R}^N, \tag{5}$$

$$N = \sum_{i=1}^{K} N_i. \tag{6}$$

Here the coefficient vector, $\mathbf{x}_0$, is sparse because the coefficients unrelated to the i-th person are zero.

To recognize faces, solution $\mathbf{x}_0$ obtained by solving Eq. (3) is essential. In this face recognition [4], Eq. (3) is typically underdetermined, $M < N$, but if optimal solution $\mathbf{x}_0$ is sufficiently sparse, $\mathbf{x}_0$ is the same as solution $\hat{\mathbf{x}}_1$ of the following ℓ^1-norm minimization problem:

$$\hat{\mathbf{x}}_1 = \min_{\mathbf{x}} \|\mathbf{x}\|_1 \text{ subject to } \mathbf{y} = \mathbf{A}\mathbf{x}. \tag{7}$$

In this method, Eq. (7) is solved after the dimension of feature vectors are reduced. Though some techniques for dimension reduction are introduced to this method [4], this paper supposes RP. By RP with random matrix $\mathbf{B} \in \mathbb{R}^{d\times M}$, feature vector $\mathbf{v}$ is projected onto a d-dimensional subspace where $d < M$. Therefore, a query vector, $\mathbf{y} \in \mathbb{R}^M$, and the set of training vectors, $\mathbf{A} \in \mathbb{R}^{M\times N}$, are projected as $\mathbf{y}' \in \mathbb{R}^d$ and $\mathbf{A}' \in \mathbb{R}^{d\times N}$, respectively:

$$\mathbf{y}' = \mathbf{B}\mathbf{y}, \tag{8}$$

$$\mathbf{A}' = \mathbf{B}\mathbf{A}. \tag{9}$$

Using Eqs. (8) and (9), Eq. (7) can be rewritten as

$$\hat{\mathbf{x}}'_1 = \min_{\mathbf{x}'} \left\|\mathbf{x}'\right\|_1 \text{ subject to } \mathbf{y}' = \mathbf{A}'\mathbf{x}'. \tag{10}$$

Finally, for the i-th person, dimension-reduced query vector $\mathbf{y}'$ is reconstructed based on Eq. (3) by using $\hat{\mathbf{x}}'_1$. Person C who minimizes the residue between $\mathbf{y}'$ and reconstructed query vector for the i-th person $\mathbf{A}\delta_i(\hat{\mathbf{x}}'_1)$ is regarded as the recognition results:

$$r_i = \left\|\mathbf{y} - \mathbf{A}\delta_i\left(\hat{\mathbf{x}}'_1\right)\right\|_2, \tag{11}$$

$$C = \arg\min_i r_i, \tag{12}$$

where $\delta_i(\hat{\mathbf{x}}')$ is the function which replaces the coefficients for training vectors unrelated to the i-th person with zeros, i.e.,

$$\delta_i\left(\hat{\mathbf{x}}'\right) = \left[0, \ldots, 0, \hat{x}'_{i,1}, \ldots, \hat{x}'_{i,N_i}, 0, \ldots, 0\right]^T. \tag{13}$$

2.2. Requirements for Template Protection Schemes

Facial templates should be protected because of privacy protection and security. The protection schemes for biometric templates such as iris, fingerprint, and facial images should satisfy the following properties [12]:

Req. (a) Diversity: The key for protecting templates should be different according to the application.

Req. (b) Revocability: If a protected template is compromised, the template can be revoked and a new protected one can be reissued from the same original facial template.

Req. (c) Security: It must be computationally hard to obtain original templates from the protected ones.

Req. (d) Performance: The template protection schemes should not degrade the recognition performance.

It is noteworthy that original templates should be held in conventional schemes to reissue protected templates when a protected template is compromised, where the key for issuing is changed.

To design a more practical recognition system, recognition systems are desired to take into account ever unconsidered requirements such as possibility of template compression and unnecessary of key management. These new requirements are of the same importance as well considered security requirements.

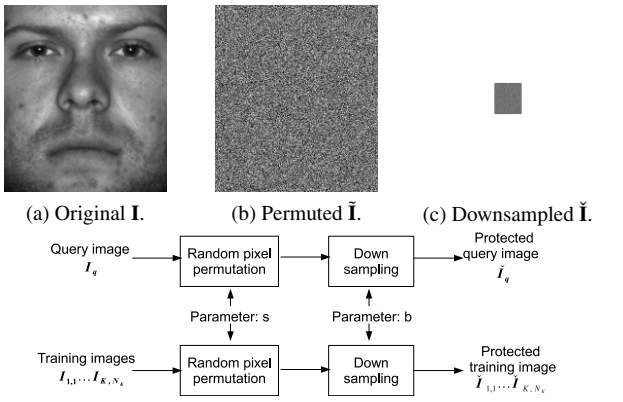


Fig. 1. The proposed template protection scheme which meets Reqs. (a) and (b).

3. PROPOSED SYSTEM

In this section, a sparse representation-based face recognition system with a new template protection scheme is proposed. Figure 1 shows the proposed template protection scheme.

3.1. Proposed Template Protection Scheme

The proposed template protection scheme consists of two steps:

Step 1. Random pixel permutation (RPP) and

Step 2. Downsampling (DS).

Steps are described in the subsequent sections.

3.1.1. Random Pixel Permutation

To visually protect original facial image $\mathbf{I} \in \mathbb{R}^{H \times W}$, pixels in $\mathbf{I}$ are randomly permuted.

$$\tilde{\mathbf{I}} = \mathrm{RndPer}\left(\mathbf{I}, s\right), \tag{14}$$

where $\tilde{\mathbf{I}} \in \mathbb{R}^{H \times W}$ is the pixel-permuted image, RndPer is the RPP function, and s is the seed for RPP, i.e., s is the first key for template protection.

3.1.2. Downsampling

To prevent an adversary from unauthorized reconstructing $\mathbf{I}$, $\tilde{\mathbf{I}}$ is downsampled to the image of size $\frac{H}{b} \times \frac{W}{b}$ as

$$\check{\mathbf{I}} = \mathrm{DownSamp}\left(\tilde{\mathbf{I}}, b\right), \tag{15}$$

where DownSamp divides the input image into $b \times b$-sized blocks and averages pixel values in each block.

3.2. Features

The features of the proposed face recognition system are summarized below.

3.2.1. Sufficient Security

The proposed scheme satisfy security requirements in Section 2.2 for template protection, whereas some of conventional systems don't satisfy all requirements [18]. The proposed system has sufficient security.

3.2.2. Efficient Compression of Protected Templates

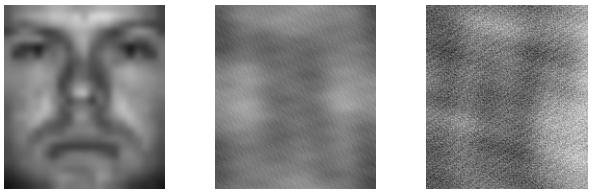
Conventional systems with protected templates need to store templates as they are because the templates are noise-like images which are not compressible. Since the histogram of protected templates is sparse in the proposed system as demonstrated later in Section 4.3, the size of templates be efficiently reduced by lossless compression techniques [19–22].

3.2.3. Key Management Free

Even if an adversary obtains a RPed template and the key for the RP from the system, c.f., Sect. 2.1, what he/she will get is protected template $\check{\mathbf{I}}$ in the proposed system. In addition, thanks to non-invertible downsampling in the proposed template protection scheme, obtaining all keys on transformations, s and b, does not help the adversary to reconstruct $\mathbf{I}$, even he/she gets $\check{\mathbf{I}}$. Thus, the keys for template protection can be disclosed to the public.

4. EXPERIMENTAL RESULTS

This section demonstrates that the proposed template protection scheme is secure (Req. (c) in Section 2.2), that the proposed face recognition system based on sparse representation [4] with the scheme keeps the recognition performance even facial images are protected (Req. (d) in Section 2.2), and that templates protected by the proposed scheme can be efficiently compressed.



(a) DS. (b) RP. (c) Proposed scheme.

Fig. 2. Images estimated from templates protected by DS, RP and proposed scheme.

4.1. Security

This section demonstrates that it is difficult to estimate the original template from the template protected by the proposed scheme. Figure 2 shows the images estimated from protected images with 504 dimension by DS, RP [13], and the proposed scheme, respectively. Figure 2 (a) is the image estimated by bilinear interpolation from protected image by DS, while Figs. 2 (b) and (c) are images estimated by the concept of compressed sensing [25] from protected image by RP and the proposed scheme, respectively. These images were estimated where transformation parameters are known.

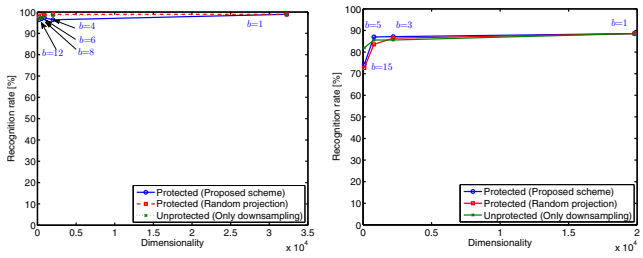
It was found that even if the transformation parameters are known, the original facial image cannot be reconstructed from the images protected by the proposed scheme and RP. Thus these schemes don't need to manage the transformation parameters, i.e., protection key, in addition to that these schemes meet Req. (c). While it was found that the scheme using only DS may not satisfy Req. (c) and need to manage transformation parameters securely.

4.2. Recognition Performance

It is demonstrated here that the proposed system is comparable to the conventional system without any template protection [4] in terms of recognition performance, even the proposed system protects templates. The conventional [4] and proposed systems were performed on Extended Yale B database [23] and AR database [24] as well as in [4]. Performances of the methods were illustrated in terms of recognition rate versus reduced dimension d.

Extended Yale B database [23] consists of 2414 frontal facial images of 38 individuals. 192×168-sized images were captured under various laboratory-controlled lightning conditions. In this section, about 64 images for each subject are randomly divided into two groups with about 32 images; one is for training and the other is for query. Fig. 3 (a) shows recognition rate versus reduced dimension d for the conventional [4] and proposed systems.

AR database [24] consists of over 4000 frontal facial images of 126 individuals where each subject participated in two sessions which separated two weeks. The size of images is



(a) Extended Yale B database [23]. (b) AR database [24].

Fig. 3. Recognition rate versus reduced dimension d for the conventional [4] and proposed systems.

165×120. In this section, a subset of the data set consisting of 50 male and 50 female subjects was used. For each subject, 14 images with various laboratory-controlled illumination conditions and facial expressions were selected. The seven images from Session 1 were used for training and the other seven images from Session 2 were used for query images in this section. Figure 3 (b) shows the results.

It was found from Fig. 3 that the proposed system is comparable to the conventional system without template protection [4] in terms of recognition performance, even the proposed system protects templates. In aadittion, the proposed system is comparable to the conventional system protected by RP [13]. Thus, it is concluded that the proposed template protection scheme satisfies Req. (d).

4.3. Compression

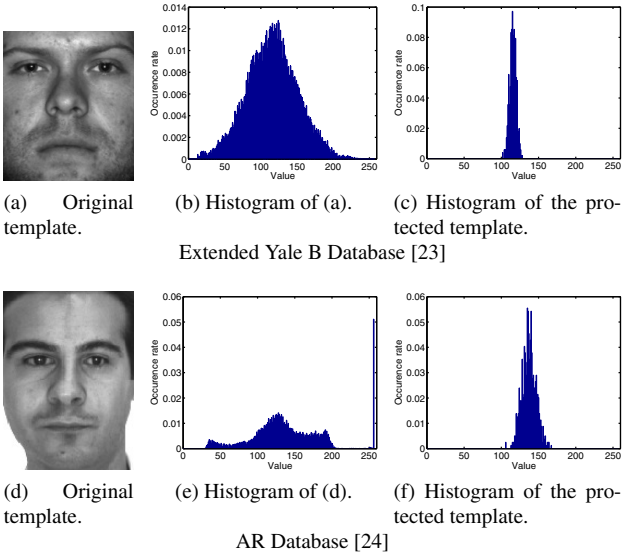
This section investigates the compression performance of templates protected by the proposed scheme. Figure 4 shows histogram of pixel values in original and protected templates. From Fig. 4, the histogram of protected template is sparser than that of original template. It has been known that images with a sparse histogram can be efficiently compressed by lossless compression techniques [19–22], and Table 1 shows the averaged data size of compressed protected templates using the proposed scheme, DS, and RP [13], respectively. Templates are compressed by JPEG-LS [27], an international standard of image compression.

From Table 1, it was confirmed that the protected template using the proposed scheme and DS can be efficiently compressed. In particular, the protected template using the proposed scheme can be compressed more efficiently than protected template using DS for small d. As large d gives weak security, it is concluded that the proposed scheme is efficient for template compression in practical scenarios.

As the conclusion of this section, Table 2 summarizes the features of various template protection schemes. From this table, it is confirmed that the proposed scheme is effective.

5. CONCLUSIONS

This paper has proposed a secure face recognition system using a new template protection scheme. The proposed scheme applies two different transformations to templates to protect



(a) Original template. (b) Histogram of (a). (c) Histogram of the protected template.

Extended Yale B Database [23]

(d) Original template. (e) Histogram of (d). (f) Histogram of the protected template.

AR Database [24]

Fig. 4. Sparse histogram of the protected template in the proposed scheme.

Table 1. Averaged data size of templates for template dimension d, measured in byte.

(a) Extended Yale B Database [23].

	Template dimension d (block size b)				
	192×168 ($b = 1$)	48×42 ($b = 4$)	32×42 ($b = 6$)	24×21 ($b = 8$)	16×14 ($b = 12$)
Proposed scheme	31414	1545	**638**	**337**	**153**
DS	**15717**	**1436**	747	476	260
RP [13]	258048	16128	10752	4032	1792

(b) AR database [24].

	Template dimension d (block size b)			
	165×120 ($b = 1$)	55×40 ($b = 3$)	33×24 ($b = 5$)	11×8 ($b = 15$)
Proposed scheme	20305	2030	684	**78**
DS	**9836**	**1453**	**644**	146
RP [13]	158400	17600	11088	704

original templates. Thanks to two applied transformations, the proposed scheme satisfies security requirements in Section 2.2. In addition, the proposed scheme can compress the protected templates efficiently by lossless compression techniques and doesn't need to manage protection keys.

Table 2. Features of template protection schemes.

	Security requirements	Key management free	Efficient compression
RPP	x	x	x
DS	x	x	o
RP [13]	o	o	x
Proposed (RPP+DS)	o	o	o

REFERENCES

[1] M.A. Turk and A.P. Pentland, "Face recognition using eigenfaces," in *Proc. IEEE CVPR*, 1991, pp.586–591.

[2] P.N. Belhumeur, J.P. Hespanha, and D.J. Kriengman, "Eigenfaces versus fisherfaces: Recogntion using class specific linear projection," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.19, pp.711–720, Jul. 1997.

[3] X. He, S. Yan, Y. Hu, P. Niyogi, and H.J. Zhang, "Face recognition using laplacianfaces," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.27, pp.328–340, Mar. 2005.

[4] J. Wright, A.Y. Yang, A. Ganesh, S.S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.31, pp.210–227, Feb. 2009.

[5] H. Kiya, S.Imaizumi, and O.Watanabe, "Partial-scrambling of image encoded using JPEG2000 without generating marker codes," in *Proc. IEEE ICIP*, 2003.

[6] O. Watanabe, A. Nakazaki, and H. Kiya, "A fast image-scramble method using public-key encryption allowing backward compatibility with JPEG2000," in *Proc. IEEE ICIP*, 2004, pp.3435–3438.

[7] S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, "Generalized hierarchical encryption of JPEG 2000 codestreams for access control," in *Proc. IEEE ICIP*, 2005, pp.II-1094–II-1097.

[8] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proc. IEEE ICIP*, 2006, pp.1977–1980.

[9] S. Imaizumi, M. Fujiyoshi, Y. Abe, and H. Kiya, "Collusion attack-resilient hierarchical encryption of JPEG 2000 codestreams with scalable access control," in *Proc. IEEE ICIP*, 2007, pp.II-137–II-140.

[10] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management," in *Proc. IEEE ICIP*, 2008, pp.269–272.

[11] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol.40, no.3, pp.614–634, 2001.

[12] A.K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol.2008, 2008.

[13] J.K. Pillai, V.M. Patel, R. Chellappa, and N.K. Ratha, "Secure and robust iris recognition using random projections and sparse representation," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.33, pp.1877–1893, Sept. 2011.

[14] A.B.J. Teoh, A. Goh, and D.C.L. Ngo, "Random multispace quantization as analytic mechanism biohashing of biometric and random identity inputs," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.28, pp.1892–1901, Dec. 2006.

[15] A.B.J. Teoh and C.T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Trans. Sys., Man, and Cybernetics Part B: Cybernetics*, vol.37, pp.1096–1106, Mon. 2007.

[16] Y.C. Feng, P.C. Yuen, and A.K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Trans. Info. Forensic Security*, vol.5, pp.103–117, Mar. 2010.

[17] M. Furukawa, Y. Muraki, M. Fujiyoshi, and H. Kiya, "A secure face recognition scheme using noisy images based on kernel sparse representation," in *Proc. APSIPA ASC*, 2013.

[18] Y. Muraki, M. Furukawa, M. Fujiyoshi, and H. Kiya, "Robustness Analysis of Cancelable Biometrics Systems in Terms of Visual Recognizability" *in Proc. The International Workshop on Advanced Image Technology*, no.A2-145, pp.24–27, Jan. 2014.

[19] P.J.S.G. Ferreira, and A.J. Pinho, "Why does histogram packing improve lossless compression rates?," *IEEE Signal Process. Letter*, vol.9, pp.–, Aug. 2002.

[20] A.J. Pinho, "An online preprocessing technique for improving the lossless compression of images with sparse histogram," *IEEE Signal Process. Letter*, vol.9, pp.–, Jan. 2002.

[21] M. Iwahashi, H. Kobayashi, and H. Kiya, "Lossy compression of sparse histogram image," in *Proc. IEEE ICASSP*, 2012, pp.1361–1364.

[22] M. Iwahashi and H. Kiya, "Two layer lossless coding of HDR images," in *Proc. IEEE ICASSP*, 2013, pp.1340–1344.

[23] A. Georghiades, P. Belhumeur, and D. Kriegman, "From few to many: Illumination cone models for face recognition under variable lightning and pose," *IEEE Trans. Pattern Analy. Mach. Intell.*, vol.23, pp.643–660, June 2001.

[24] A. Martinez and R. Benavente, "The AR face database," *CVC Tech. Rep.*, no.24, June 1998.

[25] E.J. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?," *IEEE Trans. Info. Theory*, vol.52, pp.5406–5425, Dec. 2006.

[26] R.H. Chan, C.-W. Ho, and M. Nikolova, "Salt-and-pepper noise removal by median-type noise detectors and detail-preserving regularization," *IEEE Trans. Image Process.*, vol.14, pp.1479–1485, Oct. 2005.

[27] ISO/IEC 14495–1, Information technology — Lossless and near-lossless compression of continuous-tone still images: Baseline, Dec. 1999.