Reversible Privacy Preservation using Multi-level Encryption and Compressive Sensing

Mehmet Yamaç[1], Mete Ahishali[1], Nikolaos Passalis[1], Jenni Raitoharju[1], Bulent Sankur[2], and Moncef Gabbouj[1]

[1]Tampere University, Faculty of Information Technology and Communication Sciences, Tampere, Finland
[2]Boğaziçi University, Electrical and Electronics Engineering Department, Istanbul, Turkey

***Abstract*—Security monitoring via ubiquitous cameras and their more extended in intelligent buildings stand to gain from advances in signal processing and machine learning. While these innovative and ground-breaking applications can be considered as a boon, at the same time they raise significant privacy concerns. In fact, recent GDPR (General Data Protection Regulation) legislation has highlighted and become an incentive for privacy-preserving solutions. Typical privacy-preserving video monitoring schemes address these concerns by either anonymizing the sensitive data. However, these approaches suffer from some limitations, since they are usually non-reversible, do not provide multiple levels of decryption and computationally costly. In this paper, we provide a novel privacy-preserving method, which is reversible, supports de-identification at multiple privacy levels, and can efficiently perform data acquisition, encryption and data hiding by combining multi-level encryption with compressive sensing. The effectiveness of the proposed approach in protecting the identity of the users has been validated using the goodness of reconstruction quality and strong anonymization of the faces.**

***Index Terms*—Reversible Privacy Preservation, Multi-level Encryption, Compressive Sensing, Video Monitoring**

I. Introduction

Modern intelligent buildings rely on efficient automation of various tasks ranging from traditional heating, ventilation, and air conditioning (HVAC) systems to advanced intelligent access control and monitoring systems, improving the quality of indoor environment, for example, by ensuring a higher degree of safety by hazard monitoring and by providing significant energy savings [1], [2]. However, accomplishing these tasks necessitate the installation of myriad sensors such as monitoring cameras, with concomitant privacy concerns for people living and/or working in such buildings. The recent General Data Protection Regulation (GDPR) [3] legislation in Europe reflects these concerns and regulates the ways in which sensitive data should be collected and processed, advocating data and purpose minimization principles, i.e., limiting the collected data and the information that can be inferred from them to the minimum required by the corresponding application.

These issues are currently tackled by privacy-preserving approaches that either attempt to produce an anonymized version of the original data [4], [5], namely by obfuscating the sensitive parts of the images such as faces or employ data analysis methods with strong theoretical privacy guarantees, such as differential privacy [6] or homomorphic encryption schemes [7]. However, both approaches suffer from two main handicaps, first, as they are usually non-reversible, discarding thus the original sensitive information, and second, they are costly in energy consumption and demand high-performance data processing. An ideal privacy-preserving data analysis method should a) enable reversing the de-identification for authorized users without a significant cost in terms of processing power and bandwidth, b) not degrade the non-sensitive aspects of the data so that both the semi-authorized persons can analyze the scene, e.g., for abnormal behaviour but without identifying the people via their face images and the fully authorized persons can analyze the de-obfuscated signal, c) be lightweight in energy and computational requirements.

In this work, we propose a novel and practical privacy-preserving solution for video monitoring applications such as in intelligent buildings and spaces under surveillance. Our method combines a multi-level encryption scheme with compressive sensing (CS). The proposed approach has two advantages over existing de-identification and privacy-preserving methods, namely a) it is reversible, that is, it is supporting de-identification at multiple privacy levels (as shown in Fig. 1, where different end users can get different levels of anonymized data according to the shared key, and b) it is resource and energy efficient, since it can jointly perform data acquisition, encryption, and transmission. Note that the proposed joint acquisition, privacy-protection and encryption scheme can be applied with few modifications to any kind of non-video, privacy-sensitive data.

In our method, the privacy-sensitive parts such as faces or other clues that will enable person identification for unauthorized or semi-authorized users, are obfuscated using a random corruption matrix, and then the compressed and encrypted signal is transmitted. We emphasize that compression and encryption are realized in one step via compressive sampling. The obfuscation matrix is separately encrypted and embedded into the transmitted signal. Note that the proposed method is capable of supporting multi-level de-identification, where a different level of recovery quality is provided for users at different authorization levels. The encryption, compression and embedding of the obfuscation mask into the data stream are performed in a linear fashion allowing for fast and energy efficient implementations.

978-9-0827-9703-9/19/$31.00

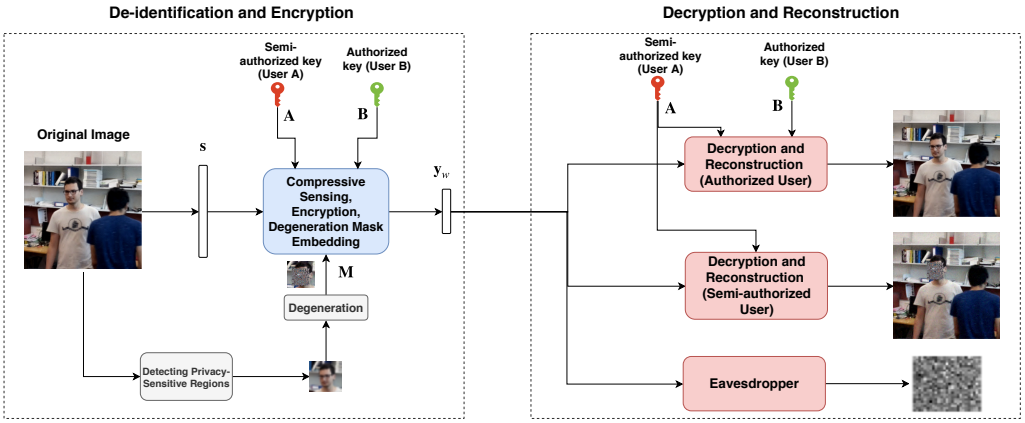

Fig. 1: Signal flow in the proposed model and illustration of the three authorization levels.

II. Background and Prior Work

CS has greatly impacted various fields of signal processing since its inception in 2005 [8]. According to the CS theory, a signal can be sampled using far fewer measurements than Nyquist-Shannon type acquisition methods. For instance, CS-based MRI imaging [9] or radar monitoring systems [10], [11] have been able to significantly reduce the signal acquisition time and bandwidth requirements over traditional approaches. In addition to data acquisition advantage, CS is inherently cryptographic [12], [13] since CS signals are linearly sampled using random measurement matrices. CS-based encryption runs thus in parallel with the data acquisition and is a low-cost solution compared to well-known complex encryption standards such as AES or RSA.

A. Compressive Sensing

Let $\mathbf{s} \in \mathbb{R}^N$ be an N-dimensional signal uniformly sampled using the traditional data acquisition scheme. In a compressive sensing scheme, this signal is linearly sampled using $m << N$ measurements, i.e.,

$$\mathbf{y} = \mathbf{A}\mathbf{s}, \tag{1}$$

where the matrix $\mathbf{A} \in \mathbb{R}^{m \times N}$ is denoted as the CS measurement matrix. It is well known that most of the signals we encounter in real life applications have some intrinsic structure, allowing for sparse sampling in some proper domain, i.e., $\mathbf{s} = \mathbf{\Phi}\mathbf{x}$, where $\mathbf{\Phi}$ is generally an $N \times N$ sparsifying basis and $\mathbf{x}$ contains the sparse coefficients with $\|\mathbf{x}\|_0 \leq k$. The underdetermined system of equations in Eq. (1) can be uniquely solved under the sparsity constraint. Using the knowledge of the sparsity or compressibility of signal decomposition in a proper domain (as given by basis $\mathbf{\Phi}$), we obtain the sparsest solution as:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_0 \quad \text{s.t.} \quad \|\mathbf{y} - \mathbf{H}\mathbf{x}\|_2 \leq \epsilon, \tag{2}$$

where $\mathbf{H} = \mathbf{A}\mathbf{\Phi}$ and ϵ is the employed threshold for solving the corresponding problem.

The optimization problem in Eq. (2) is non-convex and can be relaxed into the following ℓ_1 minimization problem:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_1 \quad \text{s.t} \quad \|\mathbf{y} - \mathbf{H}\mathbf{x}\|_2 \leq \epsilon. \tag{3}$$

The uniqueness and stability conditions of Eq. (3) are well studied in the literature. The solution of this ℓ_1 minimization problem is equal to the solution of the original ℓ_0 minimization problem in Eq. (2) if the measurement matrix A satisfies some conditions [14], [15] at the cost of an increase in the number of measurements.

B. One-class and Multi-class Encryption via Compressive Sensing

The idea of using CS in a cryptosystem was first studied in [16], where Rachlin and Baron used the CS measurement matrix as an encryption key and investigated the possibility of reconstructing the sparse coefficients $\mathbf{x}$ without the knowledge of $\mathbf{A}$. They have argued that even though it is not possible to achieve Shannon-perfect secrecy [17], it is nevertheless unfeasible for an attacker to recover information in polynomial time [16]. Then, it was proved that when the sampling matrix is i.i.d. Gaussian, then one can glean from measurement vector $\mathbf{y}$ at most information about the energy of the original signal [18], thus achieving perfect secrecy (given that, y is normalized to have a fixed energy in each transmission, the key $\mathbf{A}$ is sent in a secure channel and kept private). The robustness of the CS-based encryption was further studied in [19], where it was pointed out that even if an adversary cannot estimate the secret key $\mathbf{A}$, he/she may try to ruin the communication with additive noise attacks. However, for CS-based cryptosystems, the overall system's robustness can be satisfied to a degree even higher than that of traditional encryption schemes, provided certain necessary condition are met [19].

A multi-class encryption scheme was also proposed in [20], where the authors deliberately perturb the measurement matrix to adjust the recovery quality for different types of users by using a different measurement matrix $\mathbf{A} + \Delta\mathbf{A}$, where $\Delta\mathbf{A}$ is a partial perturbation matrix. However, their application to reversible de-identification schemes is not straightforward since the corruption induced during the de-identification stage needs to be separately transmitted in a side channel. To this effect, the work in [21], [22] introduces such a steganographic channel that enables embedding some extra information directly

on compressively sensed measurements. This steganographic channel and the resulting data hiding can allow efficient transmission of the de-identification information. Thus one can transmit encrypted and selectively obfuscated (anonymized) images with the frame-specific corruption matrix, which allows for reversing the de-identification process. Additionally, this approach further ensures the security of the system, since it is even harder for an adversary to decode the cover signal itself, given that an extra noise-like signal is added to the encrypted/compressed signal.

III. Proposed Method

We adopt the idea of using a perturbation matrix to obfuscate selectively the measurements related to the sensitive parts of images for privacy preservation. We propose a privacy-preserving method for acquiring, compressing and encrypting the information, but with the ability to reverse the de-identification so that an authorized person can recover the degraded part of the image using her key. This will be achieved without using an additional secure side channel to transmit the degradation mask. The degradation mask can be transmitted within the compressed measurements stream. On the receiver end, three levels of security are conceived. An eavesdropper not knowing the CS measurement matrix $\mathbf{A}$, (called encryption matrix in the sequel) cannot decrypt the signal. A semi-authorized person (User A) knowing $\mathbf{A}$ can decrypt the signal, while she cannot recover the privacy-preserved, i.e., the degraded parts. Finally, an authorized person (User B), who possesses the key $\mathbf{k_b}$ can extract the degradation matrix and thus, recover the full image after having reconstructed the degraded part of the signal. The proposed method is illustrated in Fig. 1.

A. Partial Perturbation of Encryption Matrix and Embedding

To conceal parts of image frames, we convert them into vectors, $\mathbf{s} \in \mathbb{R}^N$ and then define the vector indices, j, containing the privacy-sensitive sectors (this can be done manually or automatically, e.g., using face detection algorithms) and forming the set $\mathcal{C}$. We degrade the encryption matrix, $\mathbf{A}$, as

$$\tilde{\mathbf{A}} = \mathbf{A} + \mathbf{M}, \tag{4}$$

where $\mathbf{M} \in \mathbb{R}^{m \times N}$ is defined as:

$$m_{i,j} = \begin{cases} 0 \text{ with probability } p, & \text{if } j \in \mathcal{C} \quad (5a) \\ -2 * A_{i,j} \text{ with probability } 1-p, & \text{if } j \in \mathcal{C} \quad (5b) \\ 0, & \text{else.} \quad (5c) \end{cases}$$

Finally, we can encode the signal $\mathbf{s}$ with the degraded encryption matrix, $\tilde{\mathbf{A}}$, instead of $\mathbf{A}$, before broadcasting it, i.e., $\mathbf{y}_d = \tilde{\mathbf{A}}\mathbf{s}$.

The perturbation matrix, $\mathbf{M}$, can be then ternary coded into a vector $\mathbf{w} \in \mathbb{R}^T$ as:

$$w_k = \begin{cases} a, & \text{if } m_{i,\mathcal{C}_k} = 0 \text{ (for any row } i), \quad (6a) \\ -a, & \text{if } m_{i,C_k} = -2 * A_{i,\mathcal{C}_k} \text{ (for any row } i), \quad (6b) \\ 0 & \text{else,} \quad (6c) \end{cases}$$

where $\mathcal{C}_k$ is the k-th element of the set $\mathcal{C}$ and a is the selected embedding power. Note that for a system that has a total data hiding capacity of size T, $|w| \leq T$. The steganographic capacity T is dictated by the data hiding limits [21], [22]. At this stage, an embedding matrix (authorization key) $\mathbf{B} \in \mathbb{R}^{m \times T}, T < m$ is used to linearly embed the information for de-identification of the privacy-sensitive measurements directly into the encrypted signal:

$$\mathbf{y}_w = (\mathbf{A} + \mathbf{M})\mathbf{s} + \mathbf{B}\mathbf{w} = \mathbf{H}\mathbf{x} + \mathbf{B}\mathbf{w} + \mathbf{n} \tag{7}$$

where $\mathbf{x} \in \mathbb{R}^N$ is the vector of sparse coefficients of $\mathbf{s}$ in $\mathbf{\Phi}$, while the rest of the quantities are defined as $\mathbf{H} = \mathbf{A}\mathbf{\Phi}$, and $\mathbf{n} = M\mathbf{s}$. We also impose an embedding power constraint $\|\mathbf{B}\mathbf{w}\| \leq P_E$ in order not to harm the reconstruction quality for the semi-authorized users. Finally, the encrypted measurements $\mathbf{y}_w$ are transmitted/stored as shown in the Fig. 1.

B. Recovery Algorithms for Different Type of Users

A semi-authorized user (User A), who has only the key $\mathbf{A}$, can apply the ℓ_1-decoding scheme, as in Algorithm 1, to reconstruct the de-identified version of the video. The privacy-sensitive parts of the images, e.g., faces, will remain unrecognizable to user A. For the authorized users (User B), we follow the recovery method proposed in [22]. To extract $\mathbf{w}$, we first construct an annihilator matrix $\mathbf{F} \in \mathbb{R}^{P \times m}$, so that $\mathbf{F}\mathbf{B} = 0$ and $P = m - T$. We remove this embedded signal by applying $\mathbf{F}$ to $\mathbf{y}_w$:

$$\tilde{\mathbf{y}} = \mathbf{F}(\mathbf{H}\mathbf{x} + \mathbf{B}\mathbf{w} + \mathbf{n}) = \mathbf{F}\mathbf{H}\mathbf{x} + \mathbf{z}, \tag{8}$$

where $\mathbf{z} = \mathbf{F}\mathbf{n}$. Then, a pre-estimation of the sparse signal $\mathbf{x}$ can be calculated as:

$$\tilde{\mathbf{x}} = \arg\min \|\mathbf{x}\|_1 \;\; s.t. \;\; \|\tilde{\mathbf{y}} - \mathbf{F}\mathbf{H}\mathbf{x}\|_2 \leq \epsilon. \tag{9}$$

Hereafter, a pre-estimation of $\mathbf{w}$ can be found using least squares:

$$\mathbf{w}'' = (\mathbf{B}^T\mathbf{B})^{-1}\mathbf{B}^T(\mathbf{y}_w - \mathbf{H}\tilde{\mathbf{x}}). \tag{10}$$

Following this step, the 0's in the ternary message can be extracted using a simple hard thresholding to $\mathbf{w}''$, i.e., $\tilde{\mathbf{w}} = \mathbf{w}'' \odot \mathbf{1}_{|\mathbf{w}''_\mathbf{i}| > \eta}$ where $\odot$ denotes the element-wise multiplication operator between two vectors,

$$1_{|w''_i| > \eta, i} = \begin{cases} 1, & \text{if } |w''_i| > \eta, \quad (11a) \\ 0 & \text{else,} \quad (11b) \end{cases}$$

and η is the threshold value. Finally, an improved estimate of the embedded information is obtained as:

$$\hat{w}_i = a * \text{sgn}(\tilde{w}_i), \tag{12}$$

and the sparse signal is recovered as:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \; \|\mathbf{x}\|_{\ell_1^N} \quad \text{s.t.} \quad \|(\mathbf{y} - \mathbf{B}\hat{\mathbf{w}}) - (\mathbf{A} + \mathbf{M})\mathbf{\Phi}\mathbf{x}\|_{\ell_2^m} \leq \epsilon. \tag{13}$$

The recovery algorithm for the fully authorized user is provided in Algorithm 2. The recovery guarantee conditions, as well as a robustness analysis of the proposed embedding and recovery algorithm are provided in [21], [23].

Algorithm 1 Reconstruction for semi-authorized user

Input: $\mathbf{y}$, $\mathbf{A}$, $\mathbf{\Phi}$;
Hyper-parameters: ϵ
1. Estimate $\hat{\mathbf{x}}$: $\tilde{\mathbf{x}} = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_1 \quad \text{s.t.} \quad \|\mathbf{y}_w - \mathbf{H}\mathbf{x}\|_2 \leq \epsilon$
2. $\hat{\mathbf{s}} = \mathbf{\Phi}\hat{\mathbf{x}}$.
Return: $\hat{\mathbf{s}}$

Algorithm 2 Reconstruction for full-authorized user

Input: $\mathbf{y}$, $\mathbf{A}$, $\mathbf{B}$, $\mathbf{\Phi}$;
Hyper-parameters: ϵ
1. Apply $\mathbf{F}$ to $\mathbf{y}$: $\tilde{\mathbf{y}} = \mathbf{F}\mathbf{y}$
2. Estimate $\tilde{\mathbf{x}}$: $\tilde{\mathbf{x}} = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_1 \quad \text{s.t.} \quad \|\tilde{\mathbf{y}} - \mathbf{F}\mathbf{H}\mathbf{x}\|_2 \leq \epsilon$
3. Estimate $\mathbf{w}''$: $\mathbf{w}'' = (\mathbf{B}^{\mathrm{T}}\mathbf{B})^{-1}\mathbf{B}^{\mathrm{T}}(\mathbf{y} - \mathbf{H}\tilde{\mathbf{x}})$
4a. Thresholding $\mathbf{w}''$: $\hat{\mathbf{w}} = \mathbf{w}'' \odot \mathbf{1}_{|w_i''|>\eta}$
4b. Forming $\hat{\mathbf{w}}$, where $\hat{w}_i = a * \mathrm{sgn}(\tilde{w}_i)$
5. Obtain $\mathbf{M}$ from $\hat{\mathbf{w}}$.
6. $\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \|\mathbf{x}\|_1 \quad \text{s.t.} \quad \|(\mathbf{y} - \mathbf{B}\hat{\mathbf{w}}) - (\mathbf{A} + \mathbf{M})\mathbf{\Phi}\mathbf{x}\|_2 \leq \epsilon$
7. $\hat{\mathbf{s}} = \Phi\hat{\mathbf{x}}$.
Return: $\hat{\mathbf{s}}$

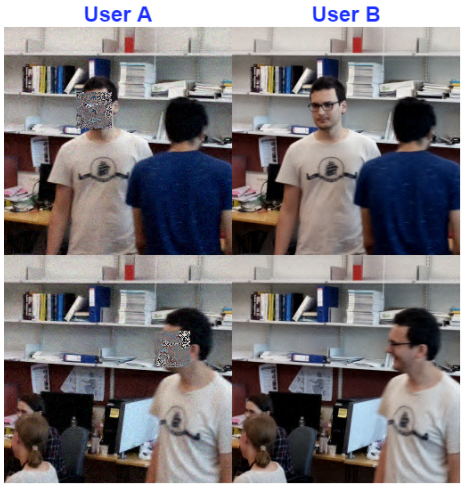

Fig. 2: Sample recovered frames for the semi-authorized (User A) and authorized (User B) (measurement rate 0.6)

C. Reversible Privacy-Preserving Video Monitoring

Random, e.g., Gaussian measurement matrices are proven to be optimal for reconstruction performances. However, direct use of the proposed approach for compressing, encrypting and transmitting video frames is practically not feasible. For example, consider a 512×512 image and a measurement rate $\frac{m}{N} = 0.36$, i.e., 90.000 measurements each demanding a different 512x512 random array, resulting in 80 gigabytes of memory. A feasible alternative for the measurement/encryption matrix consists of a matrix whose rows are randomly chosen from noiselet transform bases which are then permuted. Similarly, we pick the embedding matrix B from the DCT transform rows in the same manner as these noiselet and DCT transforms. The sparsifying basis Φ is chosen as 2-D wavelet (DWT) transform. Note that these two bases choices, namely, DWT and noiselet, are based on them being as incoherent as possible. Furthermore, recent studies [24], [25] also show that this type of CS matrix construction, i.e., choosing the rows of the matrix from a subset of the rows of a basis such as fractional Fourier, Hadamard, etc., still provides security guarantees.

IV. Experimental Evaluation

The proposed reversible privacy-preserving method is evaluated on a typical video monitoring setup that is commonly employed in such applications as analytics for intelligent buildings, video surveillance, and intelligent access control systems. We have used two video sequences (10 minutes long, a total of 3,219 frames), which were captured from two different cameras installed at Tampere University in a typical area monitoring setting. The cameras provided two different views of an office environment.

First, the ability of the proposed method to compressively sense the scene while anonymizing the detected faces and reversing the de-identification process is demonstrated in Table I. For the conducted experiments we used $T = 10000$ and a is adjusted so that we can fix the embedding power to a predetermined small value i.e., $\frac{\|Bw\|_2}{\|Ax\|_2} = 0.085$. The table reports the peak signal-to-noise ratios (PSNRs) averaged over 3,219 frames for anonymized and for clear parts of the transmitted frames. Notice that the semi-authorized user (A) receives very poorly reconstructed, practically unrecognizable face regions while the rest of the scene is well-reconstructed, only 3-5 dB worse than that of the authorized user (B). For user B, both sensitive and non-sensitive parts of the frames are well reconstructed, the sensitive parts being slightly of low quality. Two sample frames, where the information was decoded using the semi-authorized (User A) and the authorized (User B) key are shown in Fig. 2

TABLE I: Peak signal-to-noise ratios (PSNRs, dB) for anonymized and clear parts of the video frames at various measurement rates (MRs)

	Concealed Region		Outside of Concealed Region		Whole Frame	
MRs	**User A**	**User B**	**User A**	**User B**	**User A**	**User B**
0.3	10.23	21.59	24.27	26.19	21.79	25.81
0.4	9.83	26.99	26.34	29.72	22.70	29.43
0.5	9.57	31.30	28.06	33.16	23.26	32.90
0.6	9.39	34.93	29.45	36.52	23.60	36.29
0.7	9.27	38.19	30.57	39.68	23.81	39.50
0.8	9.18	40.97	31.44	42.43	23.93	42.27

We also evaluated the ability of the privacy-preserving compression method to withstand automatic recognition attacks, where a deep learning algorithm was employed to recognize the persons that appeared in the frames. To this end, we employed a state-of-the-art pre-trained Convolutional Neural Network (CNN), as provided by the dlib library [26]. The used network achieves over 99% recognition accuracy on standard Labeled Faces in the Wild benchmark dataset. For the recognition experiments, we used the pre-trained CNN to extract 128-dimensional face embeddings and query a database of known faces. Nearest neighbor search, considering the

first nearest identity was used for the classification. In all the experiments 6 different identities were used. A total of 240 face images were collected and annotated (20 frames per identity were used to form the database, while the rest of them were used for testing). The experimental results are reported in Table II. The very low recognition rate is achieved for the semi-authorized user (close to random guessing, 16.67%), while the same recognition rate as with the original frame is achieved when the measurement rate is higher than 0.6 (88.33%). Therefore, the proposed method is capable of effectively protecting the privacy of the users against a state-of-the-art recognition method when the semi-authorized key was used while allowing the authorized users to recover the sensitive information.

TABLE II: Face recognition accuracy (%) when the semi-authorized (User A) and authorized (User B) key is used. Results for different measurement rates (MRs) are reported.

MR	0.3	0.4	0.5	0.6	0.7	0.8
User A	23.33	18.33	22.50	6.67	25.00	15.83
User B	44.17	73.33	81.67	86.67	89.17	88.33

V. Conclusions

In this paper, we introduced a novel privacy-preserving compression method, which is reversible and supports de-identification at multiple privacy levels. The method can be efficiently implemented to jointly perform data acquisition, encryption, and transmission by combining multi-level encryption with compressive sensing. We implicitly assumed the availability of an ancillary technique to identify and select the privacy-sensitive part of a signal; for example, a face detector in video surveillance. The viability of the proposed approach in protecting the identity of the faces was validated using both PSNR reconstruction measure, as well as by demonstrating its robustness against automated machine learning attacks. Future work will proceed for the sequential update of the anonymized regions. More extensive testing will be carried over system parameters using open surveillance video databases. The degree of obfuscation needs to be tested also with human evaluators.

Acknowledgements

This work was supported by a NSF-Business Finland CVDI project (Amalia 3333/31/2018) and a Business Finland project VIRPA D (7940/31/2017) sponsored by Tieto Oyj, CA Technologies, and other companies.

References

[1] T. Weng and Y. Agarwal, "From buildings to smart buildings-sensing and actuation to improve energy efficiency," *IEEE Design & Test of Computers*, vol. 29, no. 4, pp. 36–44, 2012.

[2] T. A. Nguyen and M. Aiello, "Energy intelligent buildings based on user activity: A survey," *Energy and Buildings*, vol. 56, pp. 244–257, 2013.

[3] P. Voigt and A. Von dem Bussche, "The EU General Data Protection Regulation (GDPR)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[4] P. Agrawal and P. Narayanan, "Person de-identification in videos," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 3, pp. 299–310, 2011.

[5] L. Du, M. Yi, E. Blasch, and H. Ling, "Garp-face: Balancing privacy protection and utility preservation in face de-identification," in *Proceedings of the IEEE International Joint Conference on Biometrics*, 2014, pp. 1–8.

[6] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the SIGSAC Conference on Computer and Communications Security*, 2016, pp. 308–318.

[7] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 82–105, 2013.

[8] E. J. Candès *et al.*, "Compressive sampling," in *Proceedings of the International Congress of Mathematicians*, vol. 3, 2006, pp. 1433–1452.

[9] M. Lustig, D. Donoho, and J. M. Pauly, "Sparse MRI: The application of compressed sensing for rapid MR imaging," *Magnetic Resonance in Medicine: An Official Journal of the International Society for Magnetic Resonance in Medicine*, vol. 58, no. 6, pp. 1182–1195, 2007.

[10] A. C. Gurbuz, J. H. McClellan, and W. R. Scott, "A compressive sensing data acquisition and imaging method for stepped frequency GPRs," *IEEE Transactions on Signal Processing*, vol. 57, no. 7, pp. 2640–2650, 2009.

[11] M. Yamaç, M. Orhan, B. Sankur, A. S. Turk, and M. Gabbouj, "Through the wall target detection/monitoring from compressively sensed signals via structural sparsity," in *5th International Workshop on Compressed Sensing applied to Radar, Multimodal Sensing,and Imaging*, 2018.

[12] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: A survey," *IEEE Communications Surveys & Tutorials*, 2018.

[13] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.

[14] A. Cohen, W. Dahmen, and R. DeVore, "Compressed sensing and best -term approximation," *Journal of the American Mathematical Society*, vol. 22, no. 1, pp. 211–231, 2009.

[15] E. J. Candes, "The restricted isometry property and its implications for compressed sensing," *Comptes rendus mathematique*, vol. 346, no. 9-10, pp. 589–592, 2008.

[16] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proceedings of the Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 813–817.

[17] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[18] T. Bianchi, V. Bioglio, and E. Magli, "Analysis of one-time random projections for privacy preserving compressed sensing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 313–327, 2016.

[19] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proceedings of the IEEE Military Communications Conference*, 2008, pp. 1–7.

[20] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing," *IEEE Transactions on Signal Processing*, vol. 63, no. 9, pp. 2183–2195, 2015.

[21] M. Yamac, Ç. Dikici, and B. Sankur, "Hiding data in compressive sensed measurements: A conditionally reversible data hiding scheme for compressively sensed measurements," *Digital Signal Processing*, vol. 48, pp. 188–200, 2016.

[22] M. Yamaç, B. Sankur, and M. Gabbouj, "Robust data hiding scheme for compressively sensed signals," in *Proceedings of the European Signal Processing Conference*, 2018, pp. 1760–1764.

[23] M. Yamaç, Ç. Dikici, and B. Sankur, "Robust watermarking of compressive sensed measurements under impulsive and gaussian attacks," in *Proceedings of the European Signal Processing Conference*, 2013, pp. 1–5.

[24] X. Liu, W. Mei, and H. Du, "Optical image encryption based on compressive sensing and chaos in the fractional fourier domain," *Journal of Modern Optics*, vol. 61, no. 19, pp. 1570–1577, 2014.

[25] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2d compressive sensing and fractional mellin transform," *Optics Communications*, vol. 343, pp. 10–21, 2015.

[26] D. E. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, no. Jul, pp. 1755–1758, 2009.