# Year 7
# Final Project Report
# 2018-2019


**Project 7a.025.TAU – Intelligent Buildings**

A National Science Foundation
University Cooperative Research Center

# Project 7a.025.TAU – Intelligent Buildings

## Contents

## Personnel

- PI First and Last Name (PI)
    - Moncef Gabbouj
- Other team member's first and last name (project role)
    - Mehmet Yamac
    - Jenni Raitoharju (co-PI)
    - Nikolaos Passalis (co-PI)
- Sponsoring IAB member's first and last name (company name)
    - Tieto, Matti Vakkuri
    - CA Software (Technologies) Steve Greenspan

## Executive Summary/Abstract

Data plays a vital role in future intelligent buildings. Fortunately, the incoming 5-G technology will enable us to collect data continuously. Data may be collected from a variety of data sensors, such as CO2 meters, thermometers, etc., or IoT devices, such as cameras. Nevertheless, privacy protection during data collection is an important issue. For example, in a human tracking system that uses videos, we may need to hide people's faces to keep people's identify private. Our aim in this project is to create a monitoring/data collection system that protects privacy, which is energy efficient and suitable for any type of sensory signals.

## Goals and Objectives

Nowadays, constant data monitoring such as video surveillance systems has been employed everywhere, including intelligent building systems. However, at the same time, this significant increase in data collection brings some privacy concerns. Indeed, recent GDPR (General Data Protection Regulation) legislation put some regulation on privacy-preserving data collection in Europe. In addition to data privacy, in any continuous monitoring system, one of the biggest challenges is energy efficiency of sensory devices, especially in a wireless sensor network system such as wireless video surveillance systems, since sensors used in any long-term monitoring system can easily drain the battery.

In this project, we aimed to design a data monitoring system, which is a) privacy-preserving such that it anonymizes sensitive data during data collection and transmission b) energy-efficient such that it provides a low-cost data collection, compression, and an encryption scheme for sensor devices.

## Differences from Current State of Art

Typical privacy video surveillance programs insure confidentiality by anonymizing sensitive data. However, these conventional approaches have many disadvantages. For example, data anonymization is often non-reversible in these systems. Moreover, the high-level data encryption systems that provide strong security may bring a computational burden in sensory devices.

The proposed approach has three main advantages over existing anonymization techniques: a) The method provides a reversible data anonymization such that different levels of signal reconstruction is guaranteed for different types of end-users. b) It has the capacity to provide joint data acquisition, compression, encryption at sensor devices. Therefore, it enables a low-cost data collection and a transmission mechanism. c) The proposed privacy protection scheme can be applied to any types of sensory data, which includes any sensitive information.

## Methods and Datasets

The proposed method utilizes compressed sampling [1], [2], compressed encryption [3], [4] ,and direct data hiding techniques over compressed sampled signals [5], [6] .

The advantage of the CS-based technique is that the end-user can either fully recover the sampled signal or recover it in a constant manner, and on the other hand, cryptographic security can be provided.

As a case study, we developed a privacy-preserving video monitoring system. The novelty of our scheme is to provide two-level confidentiality in which the semi-authorized user, which has only a key A, will be able to recover an image which has obfuscated faces. On the other hand, the fully authorized user with two keys, A and B, is able to recover the full image. Moreover, a non-authorized user who has neither A nor B, will not be able to recover any part of the signal. A systematic representation of the proposed scheme can be seen in Figure 1.

To measure the goodness of the proposed system, we applied it to two different databases. The first database is constructed at Tampere University for this project, which we call it MUVIS (V)ideo (M)onitoring (D)atabase (MUVIS-VMD). MUVIS-VMD consist of video frames captured from two different cameras installed at Tampere University in a common working area. We used two 10 minutes long video sequences consisting of a total of 3219 frames to be evaluated. These frames include faces of 6 different identities. Furthermore, the performance evaluation was extended to a larger and more realistic public dataset, a subset of YouTube Faces Database [7], which includes 100 identities.

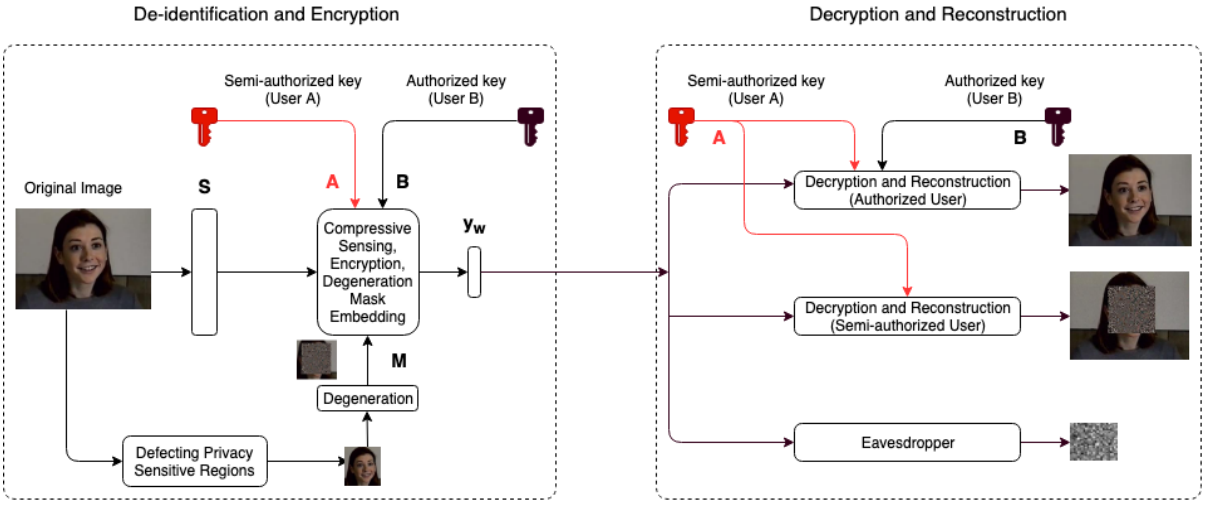

Figure 1: The proposed data collection/transmission and recovery scheme.

## Results

Compressively sensing/compression capacity can be calculated as the ratio of the dimension of the encrypted signal over that of the original signal, which we call compression ratio or measurement ratio (MR). In Figures 2 and 3, we show some examples of original signals to be encrypted, recovered signal by user A and user B for the datasets MUVIS-VMD and YouTube, respectively.


**Figure 2:** Sample recovered frames for semi-authorized (User A) and authorized (User B) for MUVIS-VMD dataset


**Figure 2:** Sample recovered frames for semi-authorized (User A) and authorized (User B) for YouTube dataset

Excessive performance evaluation on recovery and privacy preservation were made and reported in details in two submitted scientific papers in this project.

**Publications:**

1) Conference paper [8] was submitted to EUSIPCO 2019. This paper has been pre-selected as a candidate for the Student Best Paper Award.

2) Journal paper [9] was submitted to IEEE Internet of Things.

## Functionality of Innovation(s)

A novel data collection/sharing mechanism with strong privacy preserving **is** guarantee**d** at a low cost which is especially suitable for any kind of IoT device connected to a network.

## Conclusions and Recommendations

In this project, we propose a multi-layered privacy protection scheme based on compressive sensing theory. We have three user levels: A (with key A only), the semi-authorized user is only allowed to recover the non-sensitive signal, B (with key A and B) is allowed to recovery full signal, while a third-party user without the keys is not allowed to recover any piece of information.

The proposed system is low cost and practical for use in privacy-preserving data collection from sensory devices or other types of edge devices. The proposed scheme can be applied to any kind of sensory data, e.g., videos, sounds, etc. We recommend the submitted scientific papers [8] and [9] for detailed analysis and practical and theoretical aspects of the method.

## Impact and Uses/Benefits

For any kind of data collection/sharing sensory devices installed in an intelligent building, the proposed scheme provides low-cost compression, encryption, and data anonymization in data collection, sharing, and analytics.

## List of References


[1] E. J. Candès, "Compressive sampling," in *International Congress of Mathematicians, ICM 2006*, 2006.

[2] E. J. Candes and M. B. Wakin, "An Introduction To Compressive Sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, 2008.

[3] 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*. 2016.

[4] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure Wireless Communications Based on Compressive Sensing: A Survey," *IEEE Commun. Surv. Tutorials*, 2019.

[5] M. Yamaç, B. Sankur, and M. Gabbouj, "Robust data hiding scheme for compressively sensed signals," in *European Signal Processing Conference*, 2018.

[6] M. Yamaç, Ç. Dikici, and B. Sankur, "Hiding data in compressive sensed measurements: A conditionally reversible data hiding scheme for compressively sensed measurements," *Digit. Signal Process. A Rev. J.*, 2016.

[7] L. Wolf, T. Hassner, and I. Maoz, "Face recognition in unconstrained videos with matched background similarity," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2011.

[8] Yamac, Mehmet, et al. "Reversible Privacy Preservation using Multi-level Encryption and Compressive Sensing," *accepted to EUSIPCO 2019, Coruna, Spain*, 2019.

[9] Yamac, Mehmet, et al. "Multi-level Reversible Data Anonymization via Compressive Sensing and Data Hiding," *submitted to IEEE Internet of Things Journal*, 2019.