# Improvement of verification accuracy in finger vein encrypted sensing system based on compressed sensing

Hiroyuki Suzuki, Lihao Shu, Takuya Urabe, Takashi Obi, Nagaaki Ohyama
Imaging Science & Engineering Laboratory, Tokyo Institute of Technology
4259 Nagatsutacho Midoriku Yokohama, 226-8503 Japan
E-mail:hiroyuki@isl.titech.ac.jp

**Abstract** We have proposed a finger vein encrypted sensing system based on compressed sensing, in which we can acquire optically-encrypted vein images and it is possible to verify them as they are encrypted. However, its verification accuracy is not so high, whereas it can provide sufficient security enough to preserve biometric data from leaking out. To address this issue, we improve the verification method, that is, we extract the important region in the spatial frequency domain of the finger vein image. We also demonstrated the efficiency of the proposed method by numerical experiments.

**Keywords:** biometric authentication, compressed sensing, optical encryption

## 1. Introduction

In biometric authentication, it is necessary to take measures to prevent biometric information leakage, because biometric information represents some of the most important personal data, and because enrolled biometric information, unlike most personal authentication information such as passwords, cannot be altered. Correspondingly, template protection techniques for biometric authentication have been actively pursued through the development of cryptographic algorithms that protect raw biometric information obtained by a sensor while preserving high verification accuracy [1]. However, particular threats such as side channel attacks occurring while raw biometric information is being transformed into a protected template are becoming increasingly realistic. It is believed that threats such as these can be avoided by capturing optically-encrypted biometric images through image sensing.

As optical encryption techniques, double random phase encoding [2] is well-known and it has been studied extensively for two decades. On the other hand, compressed sensing (CS) [3] is also applicable to optical encryption. Based on the principle of CS, a compressive imaging (CI) system, consisting of a digital micro-mirror device (DMD) for generating random intensity patterns and a photo detector instead of an image sensor, has been proposed [4]. The CI system makes it possible to obtain an object image as hidden information by employing the observation matrix as the encryption key. In our previous study, we proposed a CI system for capturing an encrypted finger vein image and their biometric authentication schemes [5-6]. These techniques can provide sufficient security enough to preserve biometric data from leaking out. However, its verification accuracy is not so high compared with other finger vein authentication techniques. To address this issue, we improve the verification method, that is, we extract the important region in the spatial frequency domain of the finger vein image.

## 2. Encrypted sensing based on compressed sensing

Suppose that an object represented by an N-dimensional signal $\mathbf{x}=(x_1,\cdots,x_N)^T$ is observed by the CI system shown in Fig.1. A DMD generates M kinds of random binary patterns, and an M-dimensional vector $\mathbf{y}=(y_1,\cdots,y_M)^T$, which indicates the series of intensity values of the light reflected by the DMD and detected by a photo detector, is obtained as measurement data. Then, y is expressed as follows:

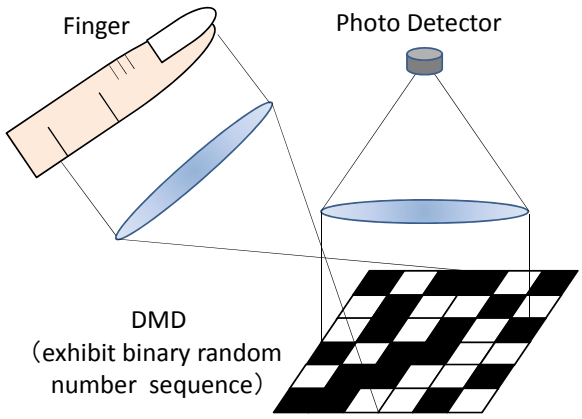


Fig. 1. CI system for capturing finger vein images.

$$\mathbf{y} = \mathbf{\Phi x}, \tag{1}$$

where $\mathbf{\Phi}$ denotes the observation matrix of the CI system.

This matrix consists of an M×N binary random number sequence. Each row denotes the random pattern exhibited in the DMD. In order to restore the objective signal x from the measurement data $\mathbf{y}$, M≥N is required in general. However, with a signal reconstruction technique based on CS, even the case M<N, can be solved with a high probability if the objective signal can be transformed into a sparse one using a linear transform, as follows:

$$\mathbf{s} = \mathbf{\Psi x}, \tag{2}$$

where $\mathbf{\Psi}$ denotes the linear transform operator. Using Eq. (1) and Eq. (2), we derive:

$$\mathbf{y} = \mathbf{\Phi\Psi}^{-1}\,\mathbf{s}, \tag{3}$$

where $\mathbf{\Psi}^{-1}$ is the inverse linear transform operator. The estimated solution of the sparse vector $\mathbf{s}$ can then be obtained by means of minimizing its L1 norm, that is:

$$\text{Minimize } ||\hat{\mathbf{s}}||_1, \quad \text{subject to } \mathbf{y} = \mathbf{\Phi\Psi}^{-1}\hat{\mathbf{s}}, \tag{4}$$

where $\hat{\mathbf{s}}$ denotes the estimated vector of $\mathbf{s}$. It is well known that L1 norm minimization can be solved by employing linear programming methods. Thus, the estimated objective signal $\hat{\mathbf{x}}$ can be obtained as follows:

$$\hat{\mathbf{x}} = \mathbf{\Phi\Psi}^{-1}\hat{\mathbf{s}}. \tag{5}$$

In this case, the matrix $\mathbf{\Phi\Psi}^{-1}$ is employed as a decryption key for the encrypted data $\mathbf{y}$.

However, the above procedure might not be secure because the original finger vein image has to be restored. In order to avoid this issue, the sparse vector $\mathbf{s}$ is randomized by the random permutation matrix $\mathbf{R}$ as follows;

$$\mathbf{R}\mathbf{s} = \mathbf{s}_r. \quad (6)$$

Using this equation, Eq. (3) can be rewritten as follows;

$$\mathbf{y} = \mathbf{\Phi}\mathbf{\Psi}^{-1}\mathbf{R}^{-1}\mathbf{s}_r. \quad (7)$$

From this equation, the randomized sparse signal $\mathbf{s}_r$ can be obtained by employing L1 norm minimization as well as Eq.(4). In this case, the matrix $\mathbf{\Phi}\mathbf{\Psi}^{-1}\mathbf{R}^{-1}$ is employed as a decryption key. This mechanism makes it possible to enhance the security of finger vein authentication because it is difficult to estimate the original finger vein image even if $\mathbf{s}_r$ is revealed to imposters.

In verification, we calculate the score of the similarity between the two randomized sparse signals on enrollment and on verification.

## 3. Improvement of verification accuracy

The proposed method described in section 2 does not perform finger vein verification with high accuracy because it uses all spatial frequency region of the finger vein image, which is sure to include unnecessary components. In order to improve the verification accuracy, we extract an important region in the spatial frequency domain which is supposed to contribute to increase of the verification accuracy. In this paper, the zero frequency (DC component) and the high frequency region are filtered, and the rest component is used for verification, as shown in Fig.2.

## 4. Numerical simulations

We conducted numerical simulations to verify finger vein images based on the proposed method. In these simulations, we used pseudo-measurement data that are generated numerically using finger vein images acquired with a commercial finger vein sensor. 2D-DCT is employed as the linear transform $\Psi$. As the criterion for verification, we employ a normalized cross correlation between the estimated sparse vectors on enrollment and on verification. In order to evaluate the verification accuracy, we carried out finger vein verifications which dealt with the case where an imposter knows the correct decryption key $\mathbf{\Phi}\mathbf{\Psi}^{-1}\mathbf{R}^{-1}$ for genuine verification. Fig. 3 shows the equal error rate (EER) depending on the number of CS measurement data. The result shows an improvement of verification accuracy compared with the conventional method which uses all spatial frequency region of the finger vein image.

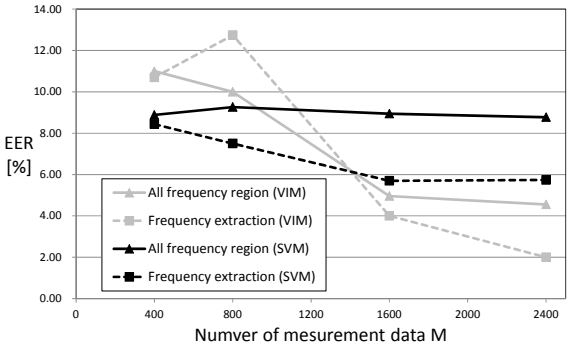


Fig. 3. Verification accuracy by numerical simulations. (VIM: Vein image matching, SVM: Sparse vector matching)

## 4. Conclusion

We presented an improved finger vein verification method based on compressed sensing, which can increase the verification accuracy by means of extracting an important region in the spatial frequency domain. With numerical simulations, we also showed that this method could improve the accuracy of the finger vein verification.

## References

[1] N. K. Ratha, J. H. Connell and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, pp. 614–634, 2001.

[2] P. Refregier and B. Javidi, "Optical Image Encryption Based on Input Plane", Opt. Lett., vol. 20, No. 7, pp. 767-769, 1995.

[3] E. J. Candès and M. B. Wakin, "Introduction to compressive sampling," in IEEE Signal Processing Magazine, vol. 25, pp. 21-30, 2008.

[4] M. B. Wakin, et al., "An Architecture for Compressive Imaging," Proc. International Conference on Image Processing (ICIP) 2006, 2006.

[5] H. Suzuki, et al. "Secure biometric image sensor and authentication scheme based on compressed sensing," Applied optics, vol. 52, no. 33, pp. 8161-8168, 2013.

[6] T. Urabe, et al. "A study on improvement of security of secure biometrics sensor based on compressed sensing," Computer Security Symposium 2013, 2D2-3, pp. 466-471, 2013 ( in Japanese).

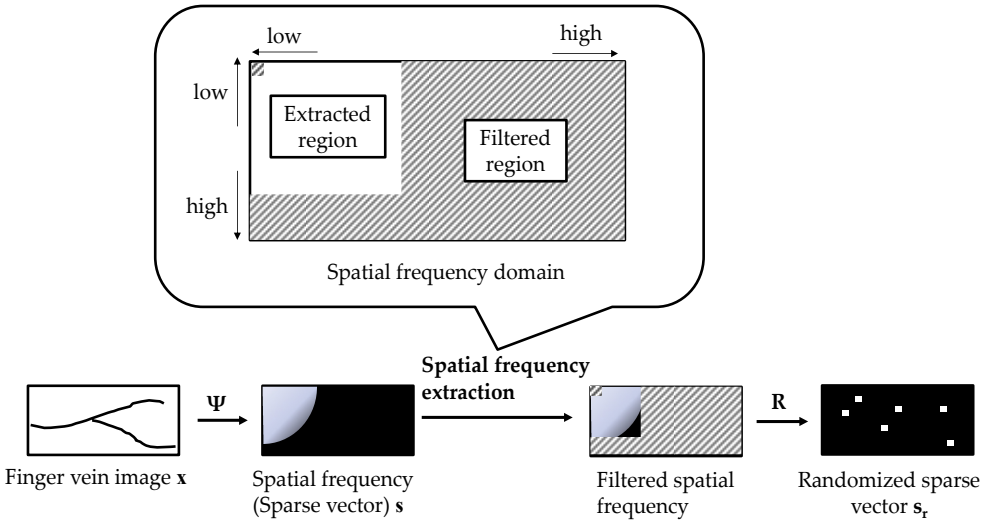


Fig. 2. Extraction of spatial frequency region.