SECURE TRANSCODING FOR COMPRESSIVE MULTIMEDIA SENSING[+]

Li-Wei Kang,[1] *Chih-Yang Lin,*[2] *Hung-Wei Chen,*[1,3] *Chia-Mu Yu,*[4] *Chun-Shien Lu,*[1,*] *Chao-Yung Hsu,*[1,3] *and Soo-Chang Pei*[3,4]

[1]Institute of Information Science, Academia Sinica, Taipei, Taiwan
[2]Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan
[3]Graduate Institute of Communication Engineering, National Taiwan University, Taipei, Taiwan
[4]Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan

ABSTRACT

Compressive sensing (CS) has recently attracted much attention due to its unique feature of directly and simultaneously acquiring compressed and encrypted data based on their sparse or compressible properties. To securely transmit compressively sensed multimedia data over networks, it is required to support transcoder to securely convert compressed multimedia into several different types for diverse receivers. In this paper, a secure transcoding scheme for compressive multimedia sensing is proposed. We focus on securely converting compressively sensed multimedia data (not data compressed via standard codec) with a certain number of measurements into other different numbers of measurements without resorting to reconstruct the original data. We show that the security can be achieved via transforming multimedia re-sensing process into another secure domain at the transcoder. We also show that the computational security can be achieved while transmitting compressively sensed data between the sender (or each receiver) and the transcoder over networks.

Index Terms**—**Secure transcoding, compressive sensing (CS), sparse representation, multimedia compression and communication.

1. INTRODUCTION

With the popularity of distribution for multimedia data over the Internet, the transcoding technique [1] has been a major core for converting the type of data transmitted from a sender to a diversity of multiple receivers equipped with different devices, such as smart phones, PDAs, notebooks, PCs, or digital TV. In such a scenario, a sender is required to send the data only once to a transcoder which can transform the data to fit a variety of capabilities or requirements, such as different bandwidths, bit rates, frame rates, resolutions, and data formats. On the other hand, multimedia data transmitted over the Internet without encryption may suffer from eavesdropping or interception, violating the copyright of the content owner. Hence, multimedia data should be compressed and encrypted prior to transmission. Traditionally, a transcoder receiving multimedia data will decrypt and decompress the data first, followed by performing re-compression and re-encryption to different types. Nevertheless, the transcoder supported by network infrastructure belongs to a third party, and, hence, such scenario cannot achieve end-to-end security since the transcoder may maliciously leak out the decrypted data.

Recently, a popular research topic is to design secure transcoding techniques [2]-[3] which can directly transcode (*e.g.*, decompress and re-compress) the received encrypted multimedia data to other data types without decrypting them. Even if decompressed encrypted data are leaked out, the original data content still cannot be recovered without accessing the secret key only available at the sender and the legal receivers.

In this paper, a secure transcoding scheme for compressive multimedia sensing is proposed. With the advancements of the compressive sensing (CS) theory [4] and the CS-based single-pixel camera architecture [5], CS has been a new data acquisition and compression paradigm based on their sparse or compressible properties [6]-[7]. To the best of our knowledge, this paper is the first to discuss (secure) transcoding for compressive multimedia sensing. The novelties include: (a) secure transcoding can be achieved via compressively re-sensing in a secure transform domain without performing complete decryption and decompression; (b) the achievable security of our scheme mainly inherits from the inherent security in CS and matrix decomposition; and (c) our scheme is fully single-pixel camera [5] compatible.

2. BACKGROUND

In order to make this paper self-contained, brief introduction of compressive sensing and sparse representation is given in this section.

2.1. Compressive Sensing

Assume that an orthonormal basis matrix (or dictionary) $\Psi \in R^{N\times N}$ (*e.g.*, DWT, *i.e.*, discrete wavelet transform, basis) can provide a K sparse representation for a real value signal $x \in R^{N\times 1}$, *i.e.*, $x = \Psi\theta$, where $\theta \in R^{N\times 1}$ can be well approximated using only $K << N$ non-zero entries. Compressive sensing (CS) [4] states that x can be accurately reconstructed by taking only $M = O(K\times log(N/K))$, $K < M << N$, linear and non-adaptive measurements from the random projection as $y = \Phi x$, where $y \in R^{M\times 1}$ is a measurement vector, $\Phi \in R^{M\times N}$ is a measurement matrix that is incoherent with Ψ. More specifically, the M measurements in y are random linear combinations of the entries of x, which can be viewed as the compressed version of x. The reconstruction of θ (or x) can be formulated as an l_1-minimization or convex unconstrained optimization problem [8]. A measurement matrix Φ can be generated randomly from some distribution controlled by a secret key. It has been shown that CS can achieve a computational notion of secrecy [9]. That is, without knowing the secret key generating Φ, it is hard to reconstruct θ from y [9]. Hence, a measurement vector y can also be viewed as an encrypted version of the original data x. On the other hand, a basis matrix (dictionary) is actually not necessarily orthonormal. An overcomplete dictionary D learned from training some selected training samples [10] can be used as a basis for representing the original data, which will be

[+]This work was supported in part by the National Science Council, Taiwan, under Grants NSC97-2628-E-001-011-MY3, NSC98-2631-H-001-013, NSC98-2811-E-001-008, NSC99-2218-E-001-010, NSC99-2811-E-001-006, and NSC99-2221-E-468-023.

[*]Corresponding author: lcs@iis.sinica.edu.tw.

978-1-4577-1302-6/11/$26.00 ©2011 IEEE

addressed in Sec. 2.2. In fact, by using a measurement matrix Φ randomly generated from some distribution, the incoherence between Φ and D should be usually high enough.

2.2. Sparse Representation

Given an overcomplete dictionary $\mathrm{D} = \left[\mathrm{d}_p\right]_{p=1,2,\ldots,P} \in \mathrm{R}^{N\times P}$, $N < P$, containing P prototype atoms $\mathrm{d}_p \in \mathrm{R}^{N\times 1}$, to find the sparse representation for a compressible signal $x\in\mathrm{R}^{N\times 1}$ as a sparsely linear combination of these atoms to meet $\|x - \mathrm{D}\alpha\|_2 \leq \varepsilon$, where $\alpha\in\mathrm{R}^{P\times 1}$ is the sparse representation coefficients of x and $\varepsilon \geq 0$ is an error tolerance, can be formulated as [10]:

$$\tilde{\alpha} = \arg\min_{\alpha}\|\alpha\|_0 \text{ subject to } \|x - \mathrm{D}\alpha\|_2 \leq \varepsilon, \tag{1}$$

where $\|\alpha\|_0$ counts the number of nonzero coefficients of α. The dimension of α is larger than that of x ($P > N$). Nevertheless, α is sparse and usually $\|\alpha\|_0 << N$. Solving Eq. (1) can also be converted into a convex optimization problem [4], [10]. By combining CS and sparse representation, a sparse or compressible signal $x\in\mathrm{R}^{N\times 1}$ being simultaneously compressed and encrypted as $y = \Phi x$ can be further expressed as $y = \Phi x = \Phi\mathrm{D}\alpha = \mathrm{A}\alpha$, where $\mathrm{A} = \Phi\mathrm{D}$ and $\mathrm{A}\in\mathrm{R}^{M\times P}$. The reconstruction of x can be formulated as a convex optimization problem as:

$$\tilde{\alpha} = \arg\min_{\alpha}\frac{1}{2}\|y - \mathrm{A}\alpha\|_2^2 + \tau\|\alpha\|_1, \tag{2}$$

and $\tilde{x} = \mathrm{D}\tilde{\alpha}$, where $\Phi\in\mathrm{R}^{M\times N}$ is a measurement matrix and τ is a non-negative parameter.

3. PROPOSED SECURE TRANSCODING FOR CS

In this section, we present the proposed secure transcoding scheme for compressive multimedia sensing. For simplicity, we will demonstrate the proposed scheme using image signals as an example, which can be naturally extended to video or other multimedia signals acquired or compressed via CS techniques. It should be noted that the proposed transcoding scheme is especially designed for CS-based multimedia compression paradigm, which is significantly different from those designed for traditional multimedia compression techniques (*e.g.*, JPEG-2000 or H.264/AVC). As shown in Fig. 1, a sender acquires an image via CS with a certain number of measurements and transmits the measurement vector (compressed image data) to a transcoder which will securely transcode the received data into L measurement vectors of different number of measurements without reconstructing the original image, and transmit these vectors to the L legal receivers accordingly.

3.1. Methodology

At the sender, an image viewed as a column vector $x\in\mathrm{R}^{N\times 1}$ can be jointly compressed and encrypted via CS using the measurement matrix $\Phi\in\mathrm{R}^{M\times N}$ (controlled by the secret key S) to get its measurement vector $y\in\mathrm{R}^{M\times 1}$, $M < N$, which is transmitted to the transcoder. The number of measurements (or the length of y) will decide the ratio for compressing x, which should be converted for fitting different requirements of multiple receivers. Here, the used measurement matrix Φ is the scrambled block Hadamard ensemble (SBHE) matrix [11], which takes the partial block Hadamard transform, followed by randomly permuting its columns.

It is assumed that the transcoder can store the (L + 1) different matrices, $\mathrm{A}\in\mathrm{R}^{M\times P}$ and $\mathrm{A}_i\in\mathrm{R}^{M_i\times P}$, i = 1, 2, …, L, where $\mathrm{A} = \Phi\mathrm{D}$, $\mathrm{A}_i = \Phi_i\mathrm{D}$, $\Phi_i\in\mathrm{R}^{M_i\times N}$ is generated using the same secret key S, $\mathrm{D}\in\mathrm{R}^{N\times P}$ is an overcomplete dictionary for sparsely representing $x = \mathrm{D}\alpha$, and $\alpha\in\mathrm{R}^{P\times 1}$ is the sparse coefficients of x, M, $M_i < N < P$, $M \neq M_i$, $M_i \neq M_j$ for $i \neq j$. Here, we apply the K-SVD algorithm [10] to learn the dictionary D using several selected training images. It should be noted that the transcoder can know only A and A_i without knowing S (or Φ and Φ_i) and D. That is, it is hard for the transcoder to correctly decompose A into Φ and D (or decompose A_i into Φ_i and D), which will be discussed in Sec. 3.2.

Because the decompression and decryption of a compressively sensed image will be jointly accomplished, for safety purpose, we cannot perform image reconstruction followed by compressively re-sensing at the transcoder. On the contrary, we propose to perform partial image reconstruction in a secure transform domain followed by re-sensing image in this domain with target number of measurements. The proposed secure transcoding scheme is illustrated in Fig. 1. In the following, we will formulate the three problems we want to solve and present corresponding solutions.

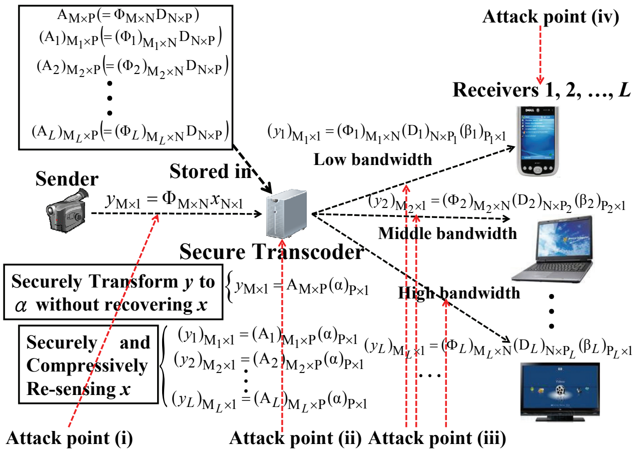
$\mathrm{A}_{\mathrm{M}\times\mathrm{P}}(=\Phi_{\mathrm{M}\times\mathrm{N}}\mathrm{D}_{\mathrm{N}\times\mathrm{P}})$
$(\mathrm{A}_1)_{\mathrm{M}_1\times\mathrm{P}}(=(\Phi_1)_{\mathrm{M}_1\times\mathrm{N}}\mathrm{D}_{\mathrm{N}\times\mathrm{P}})$
$(\mathrm{A}_2)_{\mathrm{M}_2\times\mathrm{P}}(=(\Phi_2)_{\mathrm{M}_2\times\mathrm{N}}\mathrm{D}_{\mathrm{N}\times\mathrm{P}})$
$(\mathrm{A}_L)_{\mathrm{M}_L\times\mathrm{P}}(=(\Phi_L)_{\mathrm{M}_L\times\mathrm{N}}\mathrm{D}_{\mathrm{N}\times\mathrm{P}})$
Attack point (iv)
Receivers 1, 2, …, L
$(y_1)_{\mathrm{M}_1\times 1}=(\Phi_1)_{\mathrm{M}_1\times\mathrm{N}}(\mathrm{D}_1)_{\mathrm{N}\times\mathrm{P}_1}(\beta_1)_{\mathrm{P}_1\times 1}$
Low bandwidth
Sender
Stored in
$y_{\mathrm{M}\times 1}=\Phi_{\mathrm{M}\times\mathrm{N}}x_{\mathrm{N}\times 1}$
$(y_2)_{\mathrm{M}_2\times 1}=(\Phi_2)_{\mathrm{M}_2\times\mathrm{N}}(\mathrm{D}_2)_{\mathrm{N}\times\mathrm{P}_2}(\beta_2)_{\mathrm{P}_2\times 1}$
Middle bandwidth
Secure Transcoder
Securely Transform y to α without recovering x
$y_{\mathrm{M}\times 1}=\mathrm{A}_{\mathrm{M}\times\mathrm{P}}(\alpha)_{\mathrm{P}\times 1}$
High bandwidth
Securely and Compressively Re-sensing x
$(y_1)_{\mathrm{M}_1\times 1}=(\mathrm{A}_1)_{\mathrm{M}_1\times\mathrm{P}}(\alpha)_{\mathrm{P}\times 1}$
$(y_2)_{\mathrm{M}_2\times 1}=(\mathrm{A}_2)_{\mathrm{M}_2\times\mathrm{P}}(\alpha)_{\mathrm{P}\times 1}$
$(y_L)_{\mathrm{M}_L\times 1}=(\mathrm{A}_L)_{\mathrm{M}_L\times\mathrm{P}}(\alpha)_{\mathrm{P}\times 1}$
$(y_L)_{\mathrm{M}_L\times 1}=(\Phi_L)_{\mathrm{M}_L\times\mathrm{N}}(\mathrm{D}_L)_{\mathrm{N}\times\mathrm{P}_L}(\beta_L)_{\mathrm{P}_L\times 1}$
Attack point (i)
Attack point (ii)
Attack point (iii)

Fig. 1. Proposed secure transcoding scheme for CS.

The first problem, which is secure transform to be solved at the transcoder, can be converted to solve $y = \mathrm{A}\alpha$ and formulated as a convex optimization problem shown in Eq. (2). That is, the transcoder will transform a received measurement vector y into its secure coefficient domain α for further processing. Without knowing the dictionary D, the transcoder cannot reconstruct x via $\tilde{x} = \mathrm{D}\tilde{\alpha}$. In addition, without knowing the measurement matrix Φ, the transcoder cannot reconstruct x. Hence, the solution $\tilde{\alpha}$ of Eq. (2) can be viewed as the secure sparse representation of x. Here, we apply the "sparse reconstruction by separable approximation (SpaRSA)" algorithm [8] to solve the convex optimization problem due to its superior efficiency.

The second problem, which is secure re-sensing to be solved at the transcoder, can be formulated as:

$$y_i = \mathrm{A}_i\tilde{\alpha}, \tag{3}$$

which can be implicitly further expressed as $y_i = \mathrm{A}_i\tilde{\alpha} = \Phi_i\mathrm{D}\tilde{\alpha} = \Phi_i\tilde{x}$, where $\tilde{\alpha}$ is the solution of the above-mentioned first problem. Eq. (3) implies to compressively re-sense the reconstructed x using Φ_i (controlled by S) with the number M_i of measurements. Similar to the first problem, without knowing Φ_i, the transcoder cannot reconstruct x only based on y_i. Hence, Eq. (3) can be viewed as a secure re-sensing process for x. Then, the transcoder will transmit y_i to the i-th legal receiver, $i = 1, 2, \ldots, L$.

The third problem, which is reconstruction to be solved at the i-th legal receiver, can be converted to solve $y_i = \mathrm{B}_i\beta_i$ (y_i is the solution of the above-mentioned second problem) and formulated as:

$$\tilde{\beta}_i = \arg\min_{\beta_i} \frac{1}{2}\left\|y_i - \mathrm{B}_i\beta_i\right\|_2^2 + \tau\left\|\beta_i\right\|_1, \qquad (4)$$

where $\mathrm{B}_i = \Phi_i\mathrm{D}_i$, $\mathrm{B}_i \in \mathrm{R}^{M_i \times P_i}$, $\mathrm{D}_i \in \mathrm{R}^{N \times P_i}$ is the dictionary provided by the i-th legal receiver itself, $\tilde{\beta}_i \in \mathrm{R}^{P_i \times 1}$ is the sparse coefficients of x with respect to D_i, and τ is a non-negative parameter. After receiving $y_i \in \mathrm{R}^{M_i \times 1}$, the i-th legal receiver having the secret key S will generate $\Phi_i \in \mathrm{R}^{M_i \times N}$ and provide its own dictionary D_i for sparsely representing the original image x with the corresponding coefficients $\tilde{\beta}_i$ obtained via solving Eq. (4). Then, x can be reconstructed via $\hat{x}_i = \mathrm{D}_i\tilde{\beta}_i$.

3.2. Security Analysis

To analyze the security of the proposed scheme, we will explore the possible security breach for the four attack points, (i), (ii), (iii), and (iv), shown in Fig. 1, as follows.

(i) The first possible attack point is the channel from the sender to the transcoder where the measurement vector y may be intercepted. Based on the computationally secure property of the CS [9], it is hard to reconstruct the original image x from y without knowing the measurement matrix Φ (generated by the secret key S).

(ii) The second possible attack point is the transcoder where the matrices, A and A_i, $i = 1, 2, \ldots, L$, may be intercepted. A countermeasure to this point employs the hardness of correctly decomposing the matrix $\mathrm{A} \in \mathrm{R}^{M \times P}$ into $\Phi \in \mathrm{R}^{M \times N}$ and $\mathrm{D} \in \mathrm{R}^{N \times P}$ (or decomposing A_i into Φ_i and D, M, $M_i < N < P$) without knowing the secret key S, where Φ is the highly sparse SBHE measurement matrix [11] (controlled by S) and D is learned by the K-SVD algorithm [10] where each element is normalized such that the l_2-norm of each column is fixed to 1. Consider the multiplication of two matrices, H and G, as C = H×G, where G is orthogonal and C is symmetric. It has been shown in [12]-[13] that it is impossible to exactly recover C and H when only G can be known. The hardness of correctly decomposing the matrix "A" employed in our scheme can be explained and approximately cast to that of decomposing the matrix "G." Specifically, we consider more restrictions for "A = ΦD" by letting A be orthogonal, Φ be invertible, and D be symmetric, leading to

$$\mathrm{D} = \mathrm{Z} \times \mathrm{A}, \qquad (5)$$

where Z is the inverse of Φ. Actually, the matrix $\Phi \in \mathrm{R}^{M \times N}$ is used for dimension reduction and, hence, $M < N$. Now, we consider the special case that Φ is square ($M = N$) and invertible. In addition, Φ and D are incoherent enough and, hence, A can be very close to be orthogonal.

Based on [12], it is impossible to exactly recover Z (or Φ) and D when only A can be known. Then, we relax the restrictions back to the original (more general) conditions of A, Φ, and D. This conclusion should also be valid. Hence, it is impossible to exactly recover Φ and D even if A is intercepted. The above descriptions are also valid for "$\mathrm{A}_i = \Phi_i\mathrm{D}$." In addition, it is also hard to reconstruct x without knowing D even if the sparse representation α (with respect to D) is intercepted at this point.

(iii) The third possible attack point is the channel from the transcoder to the i-th legal receiver where the measurement vector y_i, $i = 1, 2, \ldots, L$, may be intercepted. Similar to the discussions in the first attack point, it is hard to reconstruct x from y_i without knowing Φ_i (generated by the secret key S).

(iv) The fourth possible attack point is the i-th legal receiver, $i = 1, 2, \ldots, L$, where the secret key S may be maliciously disclosed, which will destroy the security of our scheme. Possible ways to mitigate the problem may include: (a) more frequently changing the secret key S as well as the matrices, A and A_i, stored in the transcoder; and (b) traitor tracing via fingerprinting techniques.

3.3. Enhancement of Received Data

After reconstructing the image x from the measurement vector y_i, the i-th receiver may further enhance the reconstructed image quality via some post-processing techniques. A recent popular sparse representation-based image super-resolution technique [14] is suitable to be integrated with our scheme for image enhancement. Consider a high-resolution version X of x and a possible operation Q projecting X to x, we have $x = \mathrm{Q}X = \mathrm{Q}\Omega\gamma$, where Q may be the combination of a blurring and a downsampling operators [14], Ω is an overcomplete dictionary for sparsely representing X by the coefficients γ. By integrating $y_i = \mathrm{B}_i\beta_i$ and $x = \mathrm{Q}\Omega\gamma$, we have

$$y_i = \mathrm{B}_i\beta_i = \Phi_i\mathrm{D}_i\beta_i = \Phi_i x = \Phi_i\mathrm{Q}X = \Phi_i\mathrm{Q}\Omega\gamma_i = \mathrm{C}_i\gamma_i, \qquad (6)$$

where $\mathrm{C}_i = \Phi_i\mathrm{Q}\Omega$ and γ_i is the sparse coefficients for representing X of the i-th receiver. If good Q and Ω can be available, we can solve Eq. (6), similar to the formulation in Eq. (4), to get the solution of γ_i, denoted by $\tilde{\gamma}_i$, followed by $X = \Omega\,\tilde{\gamma}_i$. Then, more accurate reconstruction of x can be achieved, which is our ongoing work.

4. SIMULATION RESULTS

We applied our secure transcoding scheme for transmissions of image and video data compressed by the compressive image sensing [11] and our previous distributed compressive video sensing (DCVS) [7] techniques, respectively, where each image or video frame is decomposed into several 16×16 ($N = 256$) non-overlapping blocks and each block is individually and compressively sensed. We consider a scenario that the sender transmits each image or video frame where each block is compressively sensed with M ($M/N = 50\%$) measurements to the transcoder. The transcoder securely transcodes the received data into the three types of measurement vectors y_i with the number of measurements M_i, $i = 1, 2, 3$ ($M_1/N = 15\%$, $M_2/N = 30\%$, and $M_3/N = 60\%$), respectively, and transmit them to the three respective legal receivers ($L = 3$). The i-th receiver receiving y_i uses the secret key to generate the measurement matrix Φ_i and provides its own dictionary D_i to reconstruct the received data via performing Eq. (4) block by block. For image reconstruction, the K-SVD algorithm [10] was applied to learn the dictionaries based on 10,240 randomly selected training samples (image blocks) from 10 training images. For video reconstruction using our DCVS [7], the dictionary of a key frame (intra-encoded and intra-decoded frame) was learned based on the same manner as that used for still images.

The dictionary of a CS frame (intra-encoded and inter-decoded frame) was learned using K-SVD with the training samples extracted from the neighboring reconstructed key frames. The sizes (number of atoms) of the dictionaries used in the transcoder and the *i*-th receiver, i = 1, 2, 3, were 1024, 512, 1024, and 2048, respectively. The size of dictionary will influence the reconstruction complexity solving the convex optimization problem. It is assumed that both the computational capabilities and receiver bandwidths for the 1st, 2nd, and 3rd receivers were from low to high, as illustrated in Fig. 1.

Three baseline approaches used for comparisons include: (a) the sender compresses multiple data versions itself and directly transmit them to respective receivers without relying on transcoding (denoted by "W/O transcoding"), where the overhead of the sender is very heavy; (b) the transcoder reconstructs the original data and re-sense them to multiple versions for respective receivers (denoted by "W/O security"), which is insecure; and (c) based on the inherent robustness for measurement loss of CS, the transcoder randomly drops measurements to meet the desired number of measurements of each receiver except for the 3rd receiver (denoted by "random drop"). It should be noted that the proposed scheme is designed especially for CS-based compression techniques, which is unsuitable for comparisons with existing approaches for traditional compression techniques (*e.g.*, JPEG-2000 or H.264/AVC) [1]-[3].

The reconstruction performances (PSNR in dB) at the three receivers of the evaluated four approaches are shown in Tables 1-4. It can be observed that compared with the three approaches for comparisons, the proposed scheme can keep the three advantages: (a) secure transcoding; (b) the sender needs to send data only once; and (c) the reconstruction performances are comparable. The "W/O transcoding" approach directly transmitting the data to the respective receivers reveals the upper bounds of reconstruction performances. Nevertheless, when the number of receivers greatly increases, the overhead of the sender in this approach is unacceptable. The "W/O security" approach and the proposed scheme compressively re-sense the received data from the reconstructed pixel data and the transformed secure coefficients, respectively. Basically, the two approaches, respectively, perform insecure and secure re-sensing tasks, and exhibit very similar reconstruction performances. The performances of the "random drop" approach significantly suffer from severe measurement dropping even if CS is robust to slight measurement loss. Moreover, for the 3rd receiver with higher bandwidth, which can receive more measurements (60%) than those (50%) sent from the sender, the "W/O security", "random drop," and proposed approaches cannot satisfy this receiver because the performances have been bounded by the transcoder only receiving 50% (M/N = 50%) of measurements from the sender.

5. CONCLUSIONS

In this paper, we have proposed a secure transcoding scheme for compressive multimedia sensing. The feasibility of our scheme has been verified via simulation results and security analysis. For future researches, we will provide the formal proof of the security analysis for the attack point (ii) as well as possible fingerprinting techniques for the attack point (iv) mentioned in Sec. 3.2. In addition, we will also investigate super-resolution techniques integrated with our scheme for further performance enhancement.

Table 1. Reconstruction performances for the *Lena* image.

PSNR (dB)	1st receiver	2nd receiver	3rd receiver
W/O transcoding	27.09	32.06	37.16
W/O security	27.06	31.86	34.21
Random drop	16.55	19.15	34.28
Proposed	27.07	31.75	34.27

Table 2. Reconstruction performances for the *Pepper* image.

PSNR (dB)	1st receiver	2nd receiver	3rd receiver
W/O transcoding	26.36	30.01	35.94
W/O security	26.33	29.87	33.46
Random drop	15.56	17.97	33.48
Proposed	26.35	29.82	33.43

Table 3. Reconstruction performances for the *Forman* sequence.

PSNR (dB)	1st receiver	2nd receiver	3rd receiver
W/O transcoding	23.88	25.56	27.56
W/O security	22.77	24.01	26.50
Random drop	12.56	14.91	26.59
Proposed	22.77	23.95	26.56

Table 4. Reconstruction performances for the *Coastguard* sequence.

PSNR (dB)	1st receiver	2nd receiver	3rd receiver
W/O transcoding	25.67	26.79	28.67
W/O security	24.35	25.18	27.61
Random drop	14.46	15.67	27.69
Proposed	24.29	25.17	27.67

6. REFERENCES

[1] J. Xin, C. W. Lin, and M. T. Sun, "Digital video transcoding," *Proceedings of the IEEE* vol. 93, no. 1, pp. 84-97, 2005.

[2] J. Apostolopoulos and S. Wee, "Secure media streaming and secure transcoding," chapter in *Multimedia Security Technologies for Digital Rights Management*, edited by Zeng, Yu, and Lin, Elsevier, July 2006.

[3] N. Thomas, D. Redmill, and D. Bull, "Secure transcoders for single layer video data," *Signal Processing: Image Communication*, vol. 25, no. 3, pp. 196-207, Mar. 2010.

[4] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, 2008.

[5] M. F. Duarte, et al., "Single-pixel imaging via compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, 2008.

[6] J. Romberg, "Imaging via compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 14-20, 2008.

[7] H. W. Chen, L. W. Kang, and C. S. Lu, "Dictionary learning-based distributed compressive video sensing," in *Proc. of Picture Coding Symposium*, Nagoya, Japan, 2010.

[8] S. J. Wright, R. D. Nowak, and M. A. T. Figueiredo, "Sparse reconstruction by separable approximation," *IEEE Trans. on Signal Processing*, vol. 57, no. 7, pp. 2479-2493, 2009.

[9] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. of Allerton Conf. on Communication, Control, and Computing*, 2008.

[10] M. Aharon, M. Elad, and A. M. Bruckstein, "The K-SVD: an algorithm for designing of overcomplete dictionaries for sparse representation," *IEEE Trans. on Signal Processing*, vol. 54, 2006.

[11] L. Gan, T. T. Do, and T. D. Tran, "Fast compressive imaging using scrambled Hadamard ensemble," in *Proc. of EUSIPCO*, 2008.

[12] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. of the EUROCRYPT'84 workshop on Advances in cryptology: theory and application of cryptographic techniques*, 1984.

[13] C. M. Yu, C. S. Lu, and S. Y. Kuo, "Non-interactive pairwise key establishment for sensor networks," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 3, pp. 556-569, 2010.

[14] J. Yang, J. Wright, T. Huang, and Y. Ma, "Image super-resolution via sparse representation," *IEEE Trans. on Image Processing*, Nov., 2010.