

A Secure Communication Model with Compressive-Sensed Multimedia Data

Huimin Zhao^{1,*}, Zhenzhen Pei², Qingyun Dai² and Haoran Hong³

¹*School of Computer Science, Guangdong Polytechnic Normal Univ., China*

²*School of Electronic and Information, Guangdong Polytechnic Normal Univ., China*

³*College of Information Science and Technology, Dalian Maritime University, China*

*Zhaohuimin@gpnu.edu.cn, 1548406370@qq.com, daiqy@gdut.edu.cn,
Hong.Haoran@163.com*

Abstract

For secure transmission of multimedia data into diverse receivers with different types of terminals, a compressive sensing (CS) based secure communication model (CS-SCM) is proposed. In CS-SCM, the multimedia data and sensing matrix are represented to the transcoder in the CS domain to protect the digital content. Meanwhile, the transcoder can securely transform sensed multimedia data with a certain number of CS measurements to reconstruct the original signal with a higher probability. Extensive experimental results have shown that the secure transmission and reconstruction of the multimedia signal over the network can be achieved.

Keywords: *Compressive sensing, Secure communication model, Multimedia transmission*

1. Introduction

With the increasing massive availability of multimedia data over the Internet, secure transcoding technique has become as a core for converting various types of the data before transmission from a sender to a diversity of multiple receivers equipped with different devices, such as smart phones, PDAs, notebooks, PCs, or digital TV [1]. In such scenarios, the data needs be transcoded at the sender side once, where the transcoder transforms the data to fit a sort of capabilities or requirements according to various bandwidths, frame rates, resolutions, bit rates and data formats. For privacy and data protection, secure multimedia communication is particularly emphasized where encryption is needed to avoid potential risks of interception or eavesdropping in violating the copyright of the digital content [2]. To this end, compression and encryption prior to transmission is critical for secure communication and transmission of multimedia data.

To transform the encrypted multimedia signal into other data types, secure transcoding techniques are proposed in Apostolopoulos [2] and Thomas *et al* [3], where the original signal cannot be recovered even if the decompressed encrypted signal is leaked out. However, most of the existing secure works assume that the encrypted contents are publicly available and focus on the security of the encryption pattern, while the data privacy of the target multimedia on which the secure signal recovery is performed has received little attention. Due to the advancements of its theory [4] and the corresponding single-pixel camera architecture [5], the compressive sensing (CS) has become a new data acquisition and compression paradigm based on their sparse or compressible properties [6-7]. How to apply CS into secure multimedia communication becomes a research hotspot.

In this paper, we propose a CS based secure communication model (CS-SCM) for secure multimedia communication, where CS are employed to obtain a sparse representation of the original signal and sense the sparse signal with CS measurement matrix controlled by a secure key [8-9]. The great advantage of the CS-SCM is that the compression/decompression process undertaken are efficient and generic for a wide range of applications, where the CS-based watermarking techniques is more robust and tamper-proof as compared to existing encryption approaches [10-11]. The main characteristics of the proposed CS-SCM approach can be highlighted as follows: *i)* Even without performing complete decryption and decompression in a secure transform during the process of compressive re-sensing, secure transcoding of CS-SCM can be achieved by utilizing the inherent security of the CS, and *ii)* The original signal may be reconstructed with a higher quality in CS-SCM when combining the CS measurement matrix. As a result, it has provided a generic solution for secure multimedia communications.

The rest of this paper is organized as follows. Section 2 describes the related work of CS theory and introduces the proposed CS-SCM model. Implementation of the proposed model are discussed in Section 3. Section 4 presents the related security analysis of the CS-SCM model in constructing the original signal in CS domain. Section 5 summarizes experimental results for secure multimedia transmission over the Internet. Finally, some concluding remarks are drawn in Section 6.

2. The Proposed CS-SCM Framework

In this Section, background introduction to the CS theory and sparse representation is discussed in the first two subsections, followed by the proposed CS-SCM model as detailed below.

2.1. Compressive Sensing

The CS theory [4] and [12] asserts that when a signal can be represented by a small number of nonzero coefficients, it can be perfectly recovered after being transformed by a limited number of incoherent, non-adaptive linear measurements. For a real value signal $x \in R^{N \times 1}$, we assume that an orthonormal basis matrix (or dictionary) can provide a K sparse representation for the signal, i.e., $x \in \Psi \theta$, where θ can be well approximated using only $K \ll N$ non-zero entries, and x can be highly reconstructed by $M = O(K \times \log(N/K))$, $K < M \ll N$, 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 precisely, the M measurement of y can be considered as linear combination of the entries of x . Then, we can recover θ (or x) by the l_1 -minimization or the convex unconstrained optimization with high probability [13]. A measurement matrix controlled by a secret key can be generated randomly from some distribution. It has been shown that the CS possess a secure computational notion [8] and [14]. In other words, without knowing the secret key for generating Φ , it is very difficult to reconstruct θ from y . Therefore, a measurement vector y can also be viewed as an encrypted version of the original signal x . Furthermore, an over-complete dictionary D learned from training some selected samples can be used as a basis for representing the original signal.

2.2 Sparse Representation

Assume that an over-complete dictionary $D = [d_p]_{p=1,2,\dots,p} \in R^{N \times P}$, $d_p \in R^{N \times P}$, $N < P$, contains p prototype atoms. For finding the sparse representation of a compressible digital signal $x \in R^{N \times 1}$, the CS can compose linearly these atoms to meet the

$\|x - D\alpha\|_2 \leq \varepsilon$, where $\alpha \in R^{P \times 1}$ is the x sparse representation coefficients and $\varepsilon \geq 0$ is an error tolerance. This process can be defined in [6] as:

$$\tilde{\alpha} = \arg \min_{\alpha} \|\alpha\|_0 \text{ subject to } \|x - D\alpha\|_2 \leq \varepsilon \quad (1)$$

where $\|\alpha\|_0$ indicates the number of nonzero coefficients of α . The dimension of x is less than that of α ($P > N$). Nevertheless, α is sparse and usually $\|\alpha\|_0 \ll N$. So we can combine CS and sparse representation, the signal $x \in R^{N \times 1}$ can be simultaneously compressed and encrypted as $y = \Phi x$, where y can be further expressed as $y = \Phi x = \Phi D\alpha = A\alpha$ with $A = \Phi D$ and $A \in R^{M \times P}$. Therefore, the signal x can be reconstructed, and can be formulated as a convex optimization problem as:

$$\tilde{\alpha} = \arg \min_{\alpha} \frac{1}{2} \|y - A\alpha\|_2^2 + \tau \|\alpha\|_1 \quad (2)$$

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

2.3 The Proposed CS-SCM Framework

As shown in the diagram in Figure 1, the proposed CS-SCM framework contains three main functional blocks, *i.e.*, sender (SD), transcoder (TC) and receiver (RC). For simplicity, we describe the proposed CS-SCM using image signals as an input resource in this section. Accordingly, the CS-SCM can also be extended to video or other multimedia signals acquired or compressed via the CS techniques.

Specially, the proposed CS-SCM is designed for CS-based multimedia compression paradigm, which it is greatly different from those designed for traditional multimedia compression techniques (*e.g.*, JPEG-2000 or H.264/AVC). As shown in Fig.1, the SD acquires an image data via CS with a certain number of measurements and transmits the measurement vector y (compressed image data) to the TC which will securely transcode the received y into L measurement vectors of different number of measurements, finally the TC switch these vectors to the L legal RC which reconstruct the original image.

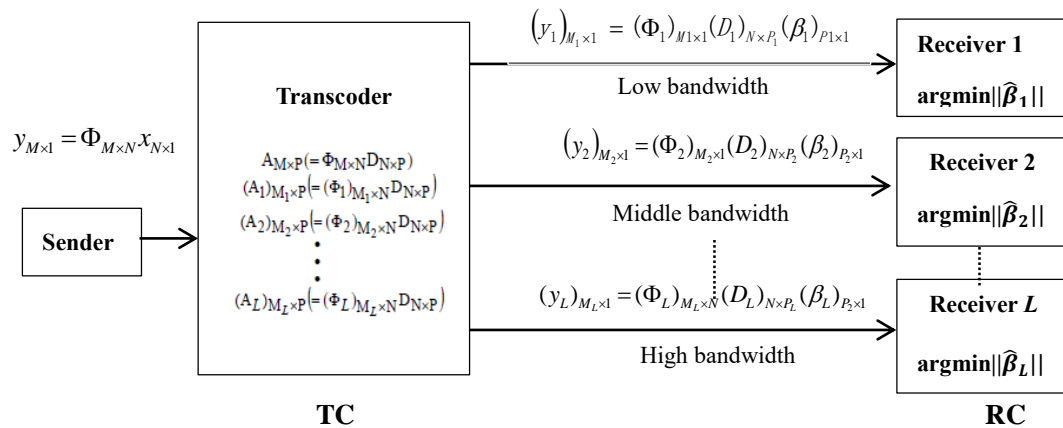


Figure 1. The Proposed CS-SCM Framework

3. The Implementation of the Proposed CS-SCM Framework

For SD, the CS uses the measurement matrix $\Phi \in \mathbb{R}^{M \times N}$ (controlled by the secret key S) to compress and encrypt a column vector $x \in \mathbb{R}^{N \times 1}$ of a signal, and obtain its measurement vector $y \in \mathbb{R}^{M \times 1}$, $M < N$, which be transmitted to the TC. In order to suit different requirement of multiple RC, the number measurement (that is the length of y) should be decided by the compressing ratio of vector x . For this reason, a scrambled block Hadamard matrix (SBHM) is used as measurement matrix Φ from our previous work in [15], which takes the partial block Hadamard transform for x , followed by randomly permuted columns.

Assuming in Figure 1 the TC in the proposed CS-SCM can store $(L+1)$ different matrices including A and A_i , where $i \in [1, L]$, $A \in \mathbb{R}^{M \times P}$ and $A_i \in \mathbb{R}^{M_i \times P}$. We have $A = \Phi D$ and $A_i = \Phi_i D$, where $\Phi_i \in \mathbb{R}^M$ is generated using the same secret key S . $D \in \mathbb{R}^{N \times P}$ is an over-complete dictionary for sparsely representing $x = D\alpha$, and $\alpha \in \mathbb{R}^{P \times 1}$ is the sparse coefficients of x , and $M, M_i < N < P, M \neq M_i, M_i \neq M_j, i \neq j$. The dictionary D is learned by using the K-SVD algorithm with the several selected training images in [16]. Actually, it should be noted that the TC of the CS-SCM can know only the A and A_i without knowing S (or Φ and Φ_i) and D . That is, the A is hard to be correctly decomposed into Φ and D (or decompose A_i into Φ_i and D) in the TC which will be discussed in Sec.4.

For security reasons, signal reconstruction is unable to be performed followed by compressively re-sensing at the TC because a compressively sensed image should be decompressed and decrypted simultaneously. Correspondingly, partial signal recovery can be achieved in a secure transform domain with target number of measurements by re-sensing image in Figure 1. In the following subsection, we will describe three secure issues to solve and present corresponding solutions in CS-SCM.

a) **The issue of secure transform at TC:** In Eq. (2), the security issue can be considered by solving $y = A\alpha$, which can be formulated as a convex optimization problem. In other words, the TC will transform a received measurement vector y into its secure coefficient domain α for further processing. The TC can't reconstruct x through $x = D\alpha$ without knowing the dictionary D , and cannot also reconstruct x without knowing the measurement matrix Φ . Therefore, the solution $\tilde{\alpha}$ can be considered as the secure sparse representation of original x . Here, the "sparse reconstruction by separable approximation (SpaRSA)" algorithm from [9] will be applied to solve the convex optimization problem due to the superior efficient of the algorithm.

b) **The issue of secure re-sensing at TC:** this can be formulated as

$$y_i = A_i \tilde{\alpha} \quad (3)$$

Eq. (3) can be further expressed as $y_i = A_i \tilde{\alpha} = \Phi_i D \tilde{\alpha} = \Phi_i \tilde{x}$, where $\tilde{\alpha}$ is sparse coefficient at the TC. From Eq.(3), the compressively re-sensing can the reconstruct signal x using Φ_i (controlled by key S) with the number M_i of measurements. Similar to the first issue, without Φ_i the TC is unable to reconstruct x only based on y_i . Therefore, Eq.(3) can be considered as a secure re-sensing process for x . Then, the TC will transmit y_i to the i -th legal receiver, $i=1,2,\dots,L$.

c) **The issue of reconstruction for the legal RC:** This can be translated to solve $y_i = B_i \beta_i$ at the i -th legal RC (y_i is the solution of the aforementioned second issue) as

$$\tilde{\beta}_i = \arg \min_{\beta_i} \frac{1}{2} \|y_i - B_i \beta_i\|_2^2 + \tau \|\beta_i\|_1 \quad (4)$$

where $\beta_i = \Phi_i D_i$, $B_i \in R^{M_i \times P_i}$, and $D_i \in R^{N \times P_i}$ is the dictionary proposed by the i -th legal RC itself, and the sparse coefficients of x is with respect to D_i , and τ is a non-negative parameter. When the i -th legal RC receives the $y_i \in R^{M_i \times N}$, then sensing matrix $\Phi_i \in R^{M_i \times N}$ will be generated using the secret key S , and the dictionary D_i will also be offered for sparsely representing the original image x with the corresponding coefficients obtained via solving Eq.(4). Finally, original signal x can be approximately reconstructed by $\tilde{x}_i = D_i \tilde{\beta}_i$.

Nevertheless, the i -th receiver may further enhance the reconstructed signal with higher quality via some post-processing. In CS-SCM, a recent popular sparse representation-based image super-resolution technique [17] is utilized to integrate the post-processing with y_i . Assuming that a high-resolution signal is X , a possible operation Q uses for projecting X to x , then we have, where Q may be the combination of a blurring and a down-sampling operators in [17], D is an over-complete dictionary for sparsely representing X by the coefficients. By integrating $y_i = B_i \beta_i$ and, the measurement vector y_i is alternated as follow:

$$y_i = B_i \beta_i = \Phi_i D_i \beta_i = \Phi_i x = \Phi_i Q X = \Phi_i Q \Omega \gamma_i = C_i \hat{\beta}_i \quad (5)$$

where Z is the sparse coefficients for representing X of the i -th receiver. To solve Eq. (5), similar strategy in Eq.(4) can be used with selected Q and D and eventually we have

$$X = D \cdot \beta \quad (6)$$

where more accurate reconstruction of x can be achieved.

4. Security Analysis

For security analysis of the proposed CS-SCM in Fig.1, the four attack points around the TC will be explored as the possible security problems as follows.

- The 1st possible attack is the channel attack between the SD and the TC, where the measurement vector y may be tampered with some illegals. According to the computationally secure property of the CS, If the measurement matrix Φ (generated by the secret key S) is unable to correctly obtain, it is difficult to recover the original image x from y .

- The 2nd possible attack is the TC attack, where the matrices A and A_i stored in TC, $i=1,2,...,L$, may have been changed. For this point, if attacker cannot know the secret key S , correctly decomposing the matrix $A \in R^{M \times P}$ into $\Phi \in R^{M \times N}$ and $D \in R^{N \times P}$, or decomposing A_i into Φ_i and D , are impossible, where matrix Φ is the highly sparse SBHM controlled by key S and D is learned by the K-SVD algorithm. On the other hand, considering the multiplication computer of matrix of SBHM, then exactly recover SBHM is impossible when A_i or Φ_i can be merely known as it has been showed in [12,13].

In CS-SCM, the hardness of correctly decomposing the matrix “ A ” is approximate to that of decomposing the matrix “ Φ ” or dictionary “ D ”. More precisely, we consider more

restrictions for “ $A = \Phi D$ ” by letting A be orthogonal, Φ be invertible, and D be symmetric, that is $D = D^T$. Where Φ^{-1} is the inverse of Φ . In fact, the matrix $\Phi \in R^{M \times N}$ is usually used to reduce signal dimension, and $M < N$. Then, the matrix Φ may be square (that is $M = N$) and invertible for the special case. In addition, Φ and D are incoherent enough CS-based theory, and A can be very approximate to be orthogonal.

According to [12], we have been known, that D or Φ are impossible to exactly be recovered when A can only be known. Even if A is intercepted by some attackers, Φ and D are impossible to exactly be recovered. This description is also valid for “ $A_i = \Phi_i D$.” At this point, even if the sparse representation α (with respect to D) is intercepted, the reconstruction x is also very hard.

- The 3rd possible attack is from channel attack between TC and RC when the TC transfers the measurement y_i , $i=1,2,...,L$ to the i -th legal RC, which may be intercepted. Similar to the first possible attack, it is difficult to reconstruct x from y_i without knowing the Φ_i (generated by the secret key S).

- The 4th possible attack can be occurred only from the i -th legal RC, $i=1,2,...,L$, where the secret key S may have been disclosed maliciously and this may destroy the proposed CS-SCM. Some possible solutions include: i) more frequently changing the secret key S and matrices A and A_i stored in the TC; and ii) digital fingerprinting techniques used in traitor.

5. Simulation Results

We applied our CS-SCM for transmissions of image and video signal compressed by the compressive image sensing [12] and our previous compressive video sensing system techniques [15], respectively. Each image or video frame is decomposed into several 8×8 non-overlapping blocks, and each block is individually and compressively sensed by block matrix of measurement matrix Φ_i . In this way, Φ_i has a block-diagonal structure as given in Eq. (7).

$$\Phi_i = \begin{bmatrix} \Phi_B & 0 & \cdots & 0 \\ 0 & \Phi_B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \Phi_B \end{bmatrix}, \quad B=8 \times 8, i=1,2,...,L \quad (7)$$

Considering a communication scenario that the SD transmits each image or video frame to the TC, each block is compressively sensed with M ($M=N/2$) measurements. In this case, the TC securely converts the received data into the various types of measurement vectors y_i by $y_i = A_i \tilde{\alpha}$ with M_i measurements, $i=1,2,...,L$, ($M_1/N=10\%$, $M_2/N=20\%$, ..., $M_L/N=80\%$), respectively. Next, the TC transmits them to the multiple different legal receivers ($L=10, 100, ..., 1000$). Finally, the i -th receiver receives y_i using the secret key S to generate the measurement matrix Φ_i and provides its own dictionary D_i to reconstruct the received data via Eq. (4) and Eq. (7) block by block.

For image signal recovery, the K-SVD algorithm [16] was applied to learn the dictionaries depending on 10,240 randomly selected training samples (image blocks) from 10 training images database. For video signal reconstruction including intra-encoded/decoded frame by using our work [15], the dictionary D_i of a key frame was learned in a similar way as that used for still images. Note that the proposed CS-SCM

is unsuitable for comparisons with existing approaches for traditional compression techniques (e.g., JPEG-2000 or H.264/AVC), the CS-SCM is only designed just for CS-based compression techniques.

In our still image based experiment, the normalized correlation (NC) is used for calculating the difference between the reconstructed signal at the RC side and the original signal at the SD side as defined below

$$NC = \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} X(i, j) \hat{X}(i, j) \quad (8)$$

where N_1 and N_2 denote the height and width of the image, respectively.

For video signal, the reconstruction quality is determined in terms of Peak Signal-to-Noise ratio ($PSNR$) between the original signal and the received signal. This process is repeated 1000 times with different key seeds S for the CS sensing matrix pattern and the average $PSNR$ is determined for comparison. The $PSNR$ can clearly indicate the quality of every received frame by comparing the degree of diversity between the received signal and the original signal. The $PSNR$ and mean square error (MSE) are expressed as

$$PSNR = 10 \log \frac{H_{\max}^2}{MSE} \quad (9)$$

$$MSE = \frac{1}{N_1 \times N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} |X(i, j) - \hat{X}(i, j)|^2 \quad (10)$$

where H_{\max} is 255 gray value for a gray-level image, N_1 and N_2 denote the height and width of the video frames, respectively.

5.1. Results for Image Communication in CS domain

We evaluate the image reconstruction performance in the proposed CS-SCM with different bit rates (BR), e.g., BR=2Mbps, 1.5Mbps, 0.5Mbps, respectively. Both the image signals and noise signals are transformed to transcoder in the CS domain.

In our experiments, the original images are obtained from a real gray level *Lena* with a size 512×512 and a fingerprint image with a size 160×160 from the FVC2004 database (DB3) [18]. Figures 2-4 show CS-based reconstruction performance as measured in NC averaged over 1000 independent RCs. As seen, no matter how BR changes, the NC values of the image recovered from our proposed CS-SCM can still exceed 0.89. However, it is almost impossible to reconstruct the images with the wrong CS matrix or without a knowing key.

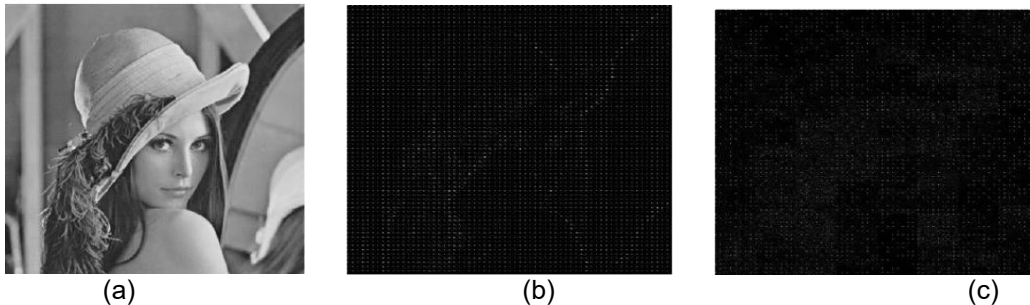




Figure 2. The Reconstruction Performance for Lina Image over BR=2Mbps Channel

(a) Original image; (b) Image in 8×8 DCT block domain; (c) DCT coefficients after CS transformation; (d) Image reconstruction with the wrong CS matrix, NC=0.08; (e) Image reconstruction with the CS matrix controlled by key, NC=0.91 and CS rate is 0.5; (f) Image reconstruction with the CS matrix controlled by key, NC=0.95 and CS rate is 0.8.

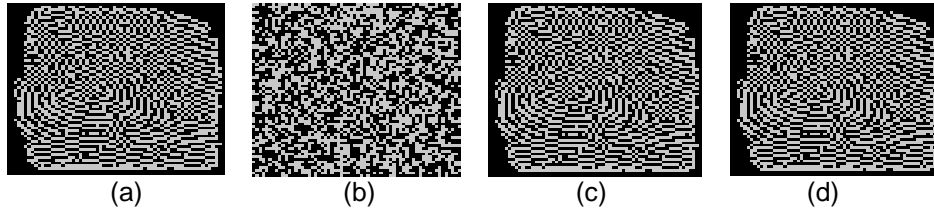


Figure 3. The Reconstruction Performance for Fingerprint Image over BR=1.5Mbps Channel

(a) Original image; (b) Image reconstruction with the wrong CS matrix, NC=0.06; (c) Image reconstruction with the CS matrix controlled by key, NC=0.89 and CS rate 0.5 is chosen; (d) Image reconstruction with the CS matrix controlled by key, NC=0.916 and CS rate 0.8 is chosen.

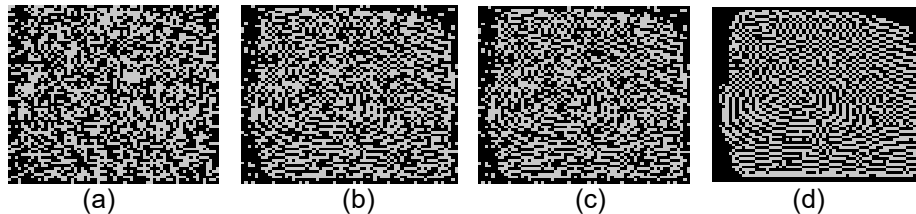


Figure 4. The Reconstruction Performance for Fingerprint Image over BR=0.5Mbps Channel

(a) Image reconstruction with the wrong CS matrix, NC=0.03; (b) Image reconstruction with the CS matrix controlled by key, NC=0.672 and CS rate 0.4 is chosen; (c) Image reconstruction with the CS matrix controlled by key, NC=0.736 and CS rate 0.5 is chosen. (d) Image reconstruction with the CS matrix controlled by key, NC=0.908 and CS rate 1.0 is chosen.

5.2. Results for Video Communication in the CS Domain

Herein we examine the performance of CS-SCM reconstruction for CS reconstruction of video signal. We use the common video sequences “Coastguard” (296 frames), “Football” (120 frames), “Hall Monitor” (88 frames), “Mobile” (296 frames), “Mother and Daughter” (296 frames), and “Stefan” (296 frames). These sequences have grayscale CIF frames of size 352×240 or 352×288 . All the video sequences are subject to block-based random projection applied frame by frame; *i.e.*, by partitioning each frame

into $B \times B = 16 \times 16$ blocks and applying to each block an orthonormalized SBHM matrix.

Here the relative performance is measured using the PSNR averaged over 1000 independent RCs at different bit rates (BR), *i.e.*, 3Mbps, 2.0Mbps, and 1.0Mbps, respectively. Figures 5-7 show the results under different BR and various CS subrates. Obviously, the six video signals can almost be reconstructed for legal 1000 RCs even though the bit rate is as low as 1.0Mbps by using the proposed CS-SCM approach.

Basically, Figures 5-7 exhibit very similar reconstruction performances. Thanks to a higher bandwidth in Fig.5, it helps to receive more measurements (60%) than those (50%) sent from the SD. However, for lower CS subrates the proposed CS-SCM approaches cannot satisfy some RCs because the performances have been bounded by the TC only receiving 50% ($M/N = 50\%$) of measurements from the SD.

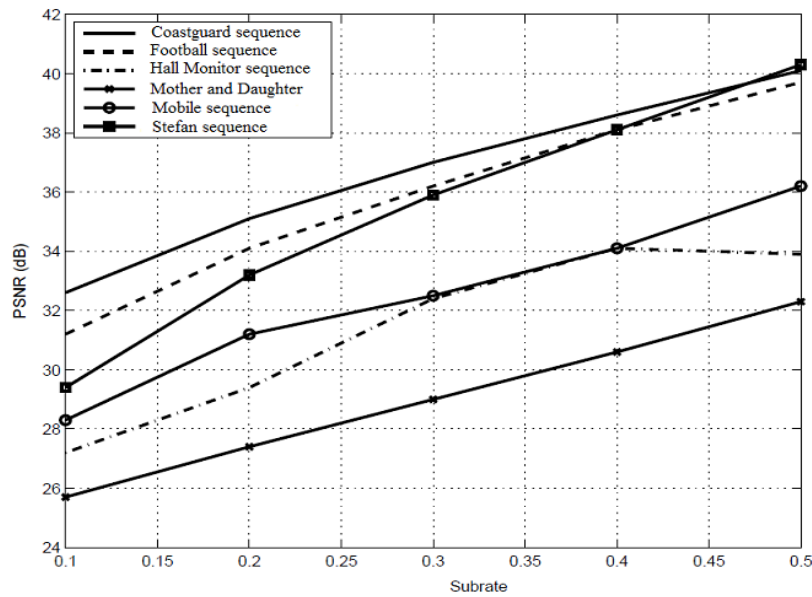


Figure 5. The Reconstruction Performance in PSNR averaged over 1000 Independent RCs for Six Sequences with BR=3.0Mbps, Respectively

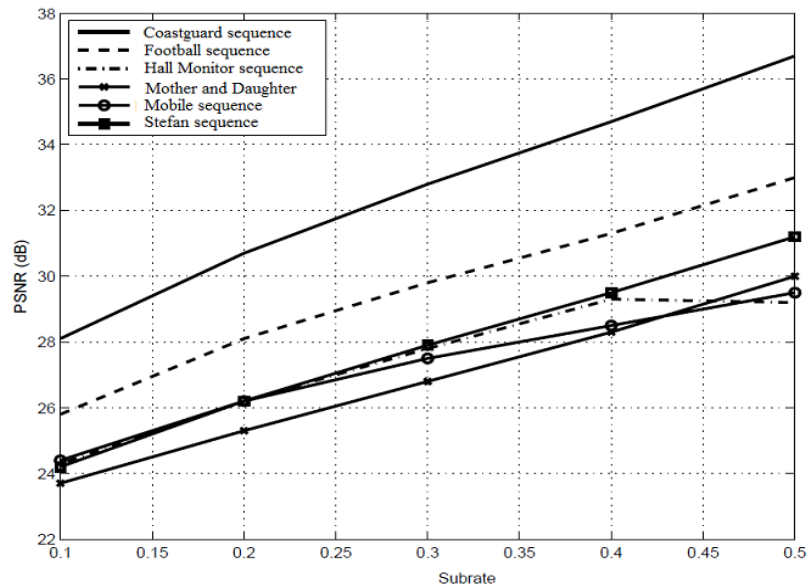


Figure 6. The Reconstruction Performance in PSNR averaged over 1000 Independent RCs for Six Sequences with BR=2.0Mbps, Respectively

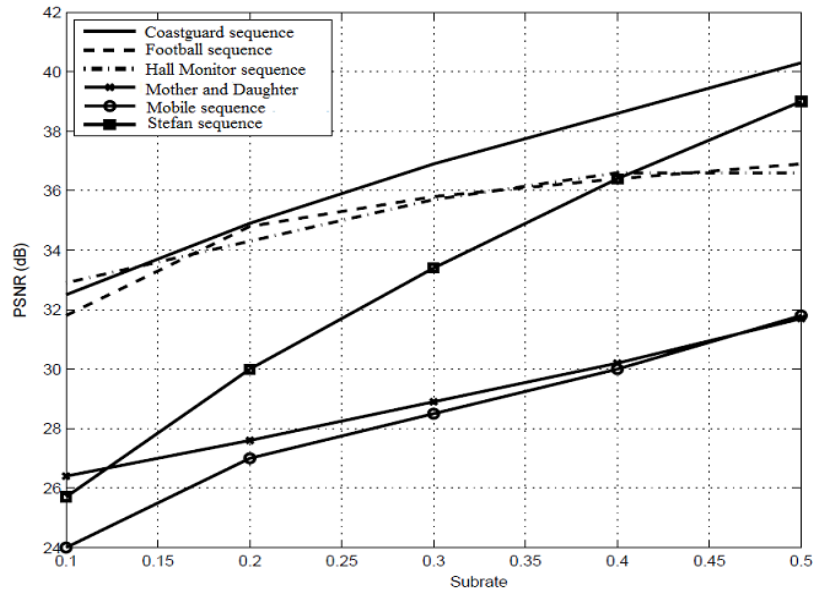


Figure 7. The Reconstruction Performance in PSNR Averaged over 1000 Independent RCs for Six Sequences with BR=1.0Mbps, Respectively

6. Conclusions

In this paper, we have proposed a CS based secure communication model (CS-SCM) with compressive-sensed multimedia data in the CS domain. We have verified the feasibility of the proposed CS-SCM with extensive simulation results and security analysis over different bit rate (BR) channels. We have demonstrated the advantages of the proposed CS-SCM framework in terms of improved quality of the reconstructed signal and enhanced security due to the CS mechanism used.

Future work will be in several ways. One is video analysis before transcoding and transmission, including video segmentation and content extraction [19-21] as well as denoising and decomposition [22-24]. In addition, object-based analysis with most state-of-the-art machine learning approaches will be highlighted as well, using deep learning and weakly-supervised learning [25-27]. Improved sparse representation with adaptive spatial support and hierarchical structuring for extra security will also be investigated [28-30].

Acknowledgments

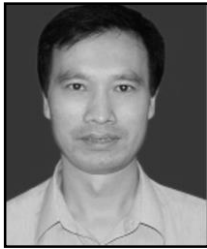
This work was supported by Guangzhou Key Laboratory of Digital Content Processing and Security Technology, and the National Natural Science Foundation of China (61672008), Guangdong Provincial Application-oriented Technical Research and Development Special fund project (2016B010127006, 2015B010131017), the Natural Science Foundation of Guangdong Province (2016A030311013, 2015A030313672), and International Scientific and Technological Cooperation Projects of Education Department of Guangdong Province (2015KGJHZ021).

References

- [1] J. Xin, C. W. Lin, and M. T. Sun, "Digital video transcoding," *Proceedings of the IEEE*, vol. 93, no. 1, (2005), pp. 84-97.
- [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, (2006).
- [3] N. Thomas, D. Redmill, and D. Bull, "Secure transcoders for single layer video data," *Signal Processing: Image Communication*, vol. 25, no. 3, (2010), pp. 196-207.

- [4] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling", IEEE Signal Processing Magazine, vol. 25, no. 2, (2008), pp: 489-509.
- [5] M. F. Duarte, "Single-pixel imaging via compressive sampling," IEEE Signal Processing Magazine, vol. 25, no. 2, (2008), pp:83-91.
- [6] J. Romberg, "Imaging via compressive sampling", IEEE Signal Processing Magazine, vol. 25, no. 2, (2008), pp. 14-20.
- [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] A. Orsdemir, H. Altun, O. G. Sharma and M. F. Bocko, "On the security and robustness of encryption via compressed sensing", IEEE Military Communications Conference, (2008), pp. 1040- 1046.
- [9] J. L. Starck, F. Murtagh and J. M. Fadili, "Sparse Image and Signal Processing: Wavelets, Curvelets", Morphological Diversity. Cambridge University Press, (2010).
- [10] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," IEEE Transaction on Information Forensics and Security, vol. 6, no. 4, (2011), pp. 1223-1232.
- [11] Q. Wang, W. Zeng, and J. Tian, "Integrated secure watermark detection and privacy preserving storage in the compressive sensing domain," IEEE International Workshop on Information Forensics and Security, Guangzhou, China, pp. 67-72.
- [12] D. L. Donoho, "Compressed sensing," IEEE Transaction on Information Theory, vol. 52, no. 4, (2006), pp. 1289-1306.
- [13] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in Proc. of Allerton Conf. on Communication, Control, and Computing, (2008), pp. 813-817.
- [14] H. Zhao and Y. M. Fang, "On the security and Robustness with Fingerprint Watermarking Signal via Compressed Sensing," Int. J. of security and Its Applications, vol. 9, no. 1, (2015), pp. 221-236.
- [15] H. Zhao and J. Ren, "Cognitive Computation of Compressed Sensing for Watermark Signal Measurement", Cognitive Computation, vol. 8, no. 2, (2016), pp. 246-260.
- [16] 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, no. 11, (2006), pp. 4311-4322.
- [17] J. Yang, J. Wright, T. Huang, and Y. Ma, "Image super-resolution via sparse representation," IEEE Trans. on Image Processing, vol. 19, no. 11, (2010), pp. 2861-2873.
- [18] Fingerprint verification competition, <http://bias.csr.unibo.it/fvc2004/>.
- [19] J. Ren, "Shot boundary detection in MPEG videos using local and global indicators", IEEE Trans. Circuits and System for Video Technology, vol. 19, no. 8, (2009), pp. 1234-1238.
- [20] J. Ren and J. Jiang, "Hierarchical modelling and adaptive clustering for real-time summarization of rush videos," IEEE Trans. Multimedia, vol. 11, no. 5, (2009), pp. 906-917.
- [21] J. Jiang, "Live: an integrated production and feedback system for intelligent and interactive broadcasting," IEEE Trans. Broadcasting, vol. 57, no. 3, (2011), pp. 646-661.
- [22] J. Ren, "High-accuracy sub-pixel motion estimation from noisy images in Fourier domain," IEEE Trans. Image Processing, vol. 19, no. 5, (2010), pp. 1379-1384.
- [23] J. Ren and T. Vlachos, "Efficient detection of temporally impulsive dirt impairments in archived films," Signal Processing, vol. 87, no. 3, (2007), pp. 541-551.
- [24] J. Zabalza, "Novel two-dimensional singular spectrum analysis for effective feature extraction and data classification in hyperspectral imaging," IEEE Trans. Geoscience and Remote Sensing, vol. 53, no. 8, (2015), pp. 4418-4433.
- [25] J. Han, "Background prior-based salient object detection via deep reconstruction residual," IEEE Trans. Circuits and Systems for Video Technology, vol. 25, no. 8, (2015), pp. 1309-1321.
- [26] J. Han, "Object detection in optical remote sensing images based on weakly supervised learning and high-level feature learning," IEEE Trans. Geoscience and Remote Sensing, vol. 53, no. 6, (2015), pp. 3325-3337.
- [27] Y. Feng, "Object-based 2D-to-3D video conversion for effective stereoscopic content generation in 3D-TV applications," IEEE Trans. Broadcasting, vol. 57, no. 2, (2011), pp. 500-509.
- [28] C. Zhao, "Improved sparse representation using adaptive spatial support for effective target detection in hyperspectral imagery," Int. J. Remote Sensing, vol. 34, no. 24, (2013), pp. 8669-8684.
- [29] P. Gao and J. Ren, "Analysis and realization of Snort-based intrusion detection system," Computer Applications and Software, vol. 23, no. 8, (2006), pp. 134-135.
- [30] Y. Zhou, "Hierarchical visual perception and two-dimensional compressive sensing for effective content-based color image retrieval," Cognitive Computation, vol. 8, no. 5, (2016), pp. 877-889.

Authors



HuiMin Zhao, was born in Shaanxi, China, in 1966. He received the B.Sc. and the M.Sc. degree in signal processing in 1992 and 1997 from Northwestern Polytechnical University, Xian, China, respectively. He received the Ph.D. degree in electrical engineering from the Sun Yat-sen University in 2001. At present, he is a professor of the Guangdong Polytechnic Normal University. His research interests include image, video and information security technology.



Qingyun Dai, received the Ph.D. degree in communication and information systems from South China University of Technology, Guangzhou, China. She is currently a Professor in the School of Information Engineering, Guangdong Polytechnic Normal University, Guangzhou, China. She has also been a Post-Doctoral Researcher at Sun Yat-sen University, Guangzhou, China. Her current research interests include Image Processing, RFID and Internet of Things.