Compressive Sensing of Medical Images With Confidentially Homomorphic Aggregations

Licheng Wang, Lixiang Li, Jin Li, Jing Li, Brij B. Gupta, and Xia Liu

Abstract—**Efficient medical image sampling and transferring becomes one of key research areas in computer science and healthcare application industries. In particular, the technique of body area networking and personal area networking are very useful in various image-based medical monitoring systems that cover a wide range of healthcare services, such as early detecting of emergency conditions and remote online instructing of surgeries. However, medical images are highly privacy sensitive and redundant. Thus, proper protection on privacy and secure data aggregation/compression are also highly expected in medical image processing. Based on compressive sensing theory, we conceive a so-called "one-stone-three-bird" solution for medical image acquisition and transmission in this paper. The size of the original medical images can be reduced to 20%, the resulted images have very well confidentiality and supporting additively homomorphic aggregation.**

Index Terms—**Compressive sensing (CS), homomorphic aggregation, medical images processing, privacy-preserving.**

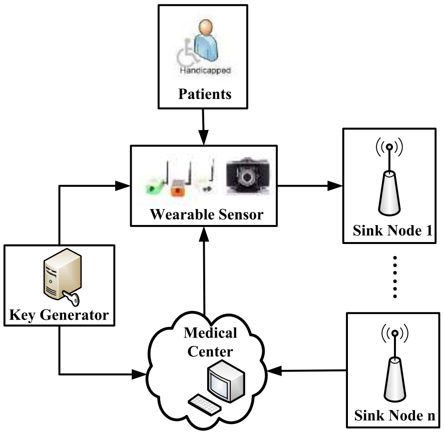

Fig. 1. Tele-medical image compression technique.

I. Introduction

A. Background

WITH the quick development of cloud computing [1], smart grid [2], big data [3], 5G cellular communication [4], context-aware networking [5], and so on, medical sensor networking technologies, including body area networking [6] and personal area networking [7], have greatly potential to change the way of living. In many individual-oriented applications, such as entertainment, travel, retail, care of the dependent people, and emergency management, the healthcare professionals or other caregivers can monitor the health condition of the children, the elderly and chronically ill based on wearable sensors. Today, these sensors can not only sampling simple signals, such as blood pressures and body temperatures but also capable of detecting unexpected motions such as falling or abrupt accelerating [8], [9]. In particular, intelligent image sensors provide good supports for remote online surgery instructing. To make these promising applications smoothing, we face the challenges coming from at least three aspects. The first is the lightweight requirement due to the energy and computation power restrictions on sensors [10], [11]. The second is the aggregation requirement since in sometimes we want to sample a common medical signal more accurately via a collaborative sensing [12]. The third is that medical singles are in general highly privacy sensitive and thus proper protection measures should be taken into account [13], [14]. Up to now, several technologies are developed to conquer these challenges. For instance, efficient image compressing methods and sparse encoding methods caters to the lightweight requirement, homomorphic encryption [15], [16] are useful for supporting data fusion and aggregation, and lightweight encryption algorithms [17] could be used to answer the challenges from both the first aspect and the third aspect.

B. Motivation

However, there are few solutions that can solve the aforementioned three challenges simultaneously. While on there are definitely requirements for this kind of integrated solutions. Let us consider the following scenario depicted in Fig. 1. In a tele-medical center, virtual endoscopic uses a camera with a micro integrated circuit sensor to obtain medical

Manuscript received January 16, 2018; revised February 20, 2018; accepted May 27, 2018. Date of publication June 7, 2018; date of current version May 8, 2019. This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800602, in part by the National Natural Science Foundation of China under Grant 61502048, and in part by the Shandong Provincial Key Research and Development Program of China under Grant 2018CXGC0701. *(Corresponding author: Jin Li.)*

L. Wang and L. Li are with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China.

J. Li and J. Li are with the School of Computer Science, Guangzhou University, Guangzhou 510006, China (e-mail: jinli71@gmail.com).

B. B. Gupta is with the Department of Computer Engineering, National Institute of Technology Kurukshetra, Kurukshetra 136119, India (e-mail: gupta.brij@gmail.com).

X. Liu is with the Shenzhen Kangning Hospital, Shenzhen Mental Health Center, Shenzhen 518003, China.

Digital Object Identifier 10.1109/JIOT.2018.2844727

images. On one hand, since some medical information are privacy sensitive, the sampled signals should be protected by some encryption algorithms. On the other hand, due to the large size of medical image, related data should be compressed/aggregated before/during the transmission to save communication bandwidth. Furthermore, to preserve the privacy of the sampled data, both the transmission and the aggregation should be fulfilled confidentially, say by using some encryption process that supporting homomorphic data fusion. A typical model for dealing with this situation might involve some wearable camera sensors that are located near by or attached to the monitoring targets (say patients), some sink nodes for image forwarding and aggregating, and a medical center for making decisions based on the collected medical image information. In this scenario, it is desirable to meet the aforementioned three requirements simultaneously. Therefore, the main motivation of this paper is to conceive a so-called "one-stone-three-bird" solution based on the newly developed compressive sensing (CS) technology.

C. Related Work

CS [18], [19] has recently emerged as a new signal sampling paradigm [20] that meets a nearly optimal Nyquist sampling rate. In the process of signal sampling, we can achieve the same effect as full sampling with few sampling points. This technology reduce the sampling points by utilizing the innatural redundance of the traditional signals, such as images and videos. By using CS technique, signals with redundance are sampled and compressed simultaneously, and the resulted signals can be reconstructed in an approximately accurate manner, from far fewer measurements than the number of unknowns [21]. Recently, CS has made major breakthroughs from both the theoretical aspects and the engineering application aspects. Different from other compressing methods such as deduplication [1], [22], CS has an advantage in some of the slower sampling situations, such as magnetic resonance imaging (MRI) in medicine, where slow sampling speed is a major drawback. After using CS technology, the original picture can be reconstructed by sampling only a fraction of the data. In this way, the sampling speed can be improved several times, and the image quality is not affected.

In light of security requirements, Huang and Sakurai [23] made the best of the characteristics of CS, and proposed a compression-combined digital image encryption method which afford to resist against consecutive packet loss and malicious shear attack. Subsequently, George and Patttathil [24] presented a novel approach for secure CS of images based on multiple 1-D chaotic maps. The basic idea of this scheme is to generate a random measurement matrix by two 1-D chaotic maps. In the same year, George and Pattathil [25] proposed another approach for generating the secure measurement matrix for CS based on linear feedback shift register (LFSR), where the basic idea is to select the different states of LFSR as the random entries of the measurement matrix and normalize these values to get independent and identically distributed random variables. However, these encryption schemes of images based on CS usually use the entire measurement matrix as the secret key, which is too large to distribute and store. To overcome this difficulty, Zhou *et al.* [26] proposed a new image compression–encryption hybrid algorithm to realize compression and encryption simultaneously by using random measurement matrices that were constructed via circulant matrices and logistic maps. Zhang *et al.* [27], [28] proposed a joint quantization and diffusion scheme based on the distribution of measurements of nature images sensed by structurally random ensemble, and an image encoding scheme for simultaneous encryption and compression based on random convolution and random subsampling. To enhance the security level and the performance of CS, Liu *et al.* [29] presented a block CS (BCS) scheme by using double random phase encoding, which is a chaos-based random phase encoding in fractional Fourier domain for each image block. To enable the block cipher structure work efficiently in the parallel computing environment, Huang *et al.* [30] proposed a encryption scheme utilizing compressive sampling that working in the parallel structure. However, in the existing BCS schemes, we adopted the same sampling rate for all the blocks. This construction may lead to the undesirable result: after subsampling, significant blocks lose may lead to some more-useful information lose while insignificant blocks still retain some less-useful information. Motivated by this observation, Zhang *et al.* [31] proposed a scalable encryption framework based on BCS along with the so-called Sobel edge detector and cascade chaotic maps.

For medical images and remote sensing satellite images, encryption is an important and sometimes a compulsory requirement to guarantee the security and privacy during the image transmission over wireless networks. Although in 2008 Rachlin and Baron [32] proved that the encryption system based on CS does not have absolute security in the ciphertext-only attack, it indeed provides certain degree protection on confidentiality in the sense that the attackers face the challenge of high computational complexity in breaking the security of the CS-based schemes. Subsequently, a series of image encryption schemes based on CS were proposed. Venkatraman and Makur [33] proposed a new method of combining decompression with decryption. Huang and Sakurai [23] proposed an image encryption method that supports noise-resistent and compression. Zhou *et al.* [34] gave a compression–encryption hybrid algorithm based on measurement matrix controlling. Yang *et al.* [35] combined the CS and blind source separation technology to construct an image encryption scheme.

Besides, chaotic systems have been widely used in image protecting based on their unpredictability and sensitivity to initial inputs. In an image encryption algorithm based on chaotic maps, the sensing matrix is generated using chaotic sequence, and it is just the symmetric key. Zhou *et al.* [36] built two secure chaotic image encryption schemes where the quantization process can be ignored. Zhang *et al.* [27] proposed a joint quantization and diffusion method based on the similarities between quantizing error feedback and cryptographic diffusion primitive. Recently, Xie *et al.* [13] provided an efficient privacy-preserving scheme based on CS to protect the privacy of transmitted data in the network.

D. Contributions

In this paper, we propose an efficient CS scheme for medical image sampling and confidentially transmission and aggregation. Our scheme answers the aforementioned three kinds of challenges simultaneously due to the following promising features.

1) A remarkable compressing ratio (about 20%) with acceptable accuracy, PSNR $\geq$ 55 dB, in the reconstructed images.
2) An observable confidentiality level (with optimal entropies) of the compressed/encrypted images.
3) An efficient additively homomorphic aggregation method over the compressed/encrypted images.

To support our claims merits, a case study has been conducted on three sets of MRI images of a brain that are scanned from the angles of horizontal, coronal, and sagittal, respectively.

Compared to the aforementioned compressed methods, our method supports confidential image aggregation, and thus meets the requirement of privacy-preserving. Compared to existing confidential aggregation methods based on homomorphic encryptions, our proposal supports image compression, and thus has lower ciphertext expansion ratio. In fact, the size of compressed/encrypted images in our proposal shrinks at a ratio 20%, while for most of homomorphic encryption schemes based on number theory or lattice, we have to put up with double or even large ciphertext expansion ratios. Note that our method also faces two limitations. The first is that our proposal works in a symmetric manner, while an asymmetric scheme is more desirable over the Internet. Another limitation is that the NPCR score of our method is a bit far from the ideal value.

E. Roadmap

The remain contents are organized as follows. Related preliminaries on CS and tent chaotic map are introduced in Section II. Our main contribution, i.e., the proposed CS scheme is described in Section III. In Section IV, the performances and the security of our proposal are manifested by testing on three sets of MRI braid images that are continuously scanned. Concluding remarks are given in Section V.

II. Preliminaries

Definition 1 (Compressed Sensing [19]): Compressed sensing is to compress an N-dimensional signal $\vec{x}$ to an M-dimensional signal vector $\vec{y}$, where $M \ll N$. Let Φ be a measurement matrix. Then

$$\vec{y} = \Phi\vec{x}. \tag{1}$$

Based on the knowledge of linear algebra, (1) is less determined. To reconstruct $\vec{x}$ from $\vec{y}$, $\vec{x}$ needs to be sparse before compression and Φ must have some special properties. Previous researches present that any N-dimensional discrete signal can be transformed into a sparse signal using a suitable basis [37], at the same time, if matrix Φ meets the restricted isometry property, then $\vec{x}$ can be reconstructed with overwhelming probability [37]. Fig. 2 shows the principle of CS and measurement process. Furthermore, chaotic functions (e.g., logistic map and Chebyshev map) are widely used to generate sensing matrices [38].

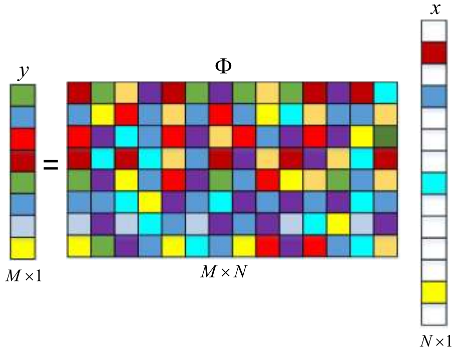

Fig. 2. Principle of CS.

Definition 2 (Skew Tent Map [39]): A skew tent map is defined as

$$z_{n+1} = \begin{cases} \dfrac{z_n}{u}, & \text{if } 0 \leq z_n \leq u \\ \dfrac{1 - z_n}{1 - u}, & \text{if } u \leq z_n \leq 1 \end{cases} \tag{2}$$

for $n = 0, 1, \ldots$, where u denotes control parameter, z_n denotes state variable. When the control parameter satisfies $u \in (0, 1)$, the system is in the chaotic state.

It can be seen from the parameter range that the variable density of the skew tent map is more stable than the logistic map, and its density function obeys uniform distribution. These advantages provide security guarantee for compressed sensing algorithms. Thus, we use skew tent map to produce the sensing matrix in this paper.

The following theorem is the theoretical basis of this paper.

Theorem 1 (OMP With Gaussian Measurements [40]): For $\delta \in (0, 0.36)$ and $N \geq K \cdot m \cdot \ln(d/\delta)$, suppose that $\vec{s}$ is an m-sparse signal in $\mathbb{R}^d$. Draw N measurements vectors $\vec{x}_1, \ldots, \vec{x}_N$ independently from standard Gaussian distribution on $\mathbb{R}^d$. Then, OMP method can reconstruct the signal $\vec{s}$ from the given N inner products $\{\langle \vec{s}, \vec{x}_i \rangle\}_{i=1}^{N}$ with probability exceeding $1 - 2\delta$.

III. Medical Image Compression Scheme

Fig. 3 illustrates the block diagram of our proposal, which focuses on implementing real-time, resource efficient and secure medical image sampling, compression/encryption, transmission, aggregation and reconstruction in a unified framework. The system mainly consists of three parts in the encryption process, i.e., the quantization process, the new CS algorithm, and the aggregation process. The corresponding inverse operations in the reverse order are executed in the decryption/reconstruction process.

The new proposed scheme consists of four phases as follows.

1) *Phase 1:* Sensor 1 collects medical images $A_1, \ldots, A_n$, then sends them to the next node—sensor 2.[1]

[1] In a collaborative sensing scenario, both sensor 1 and sensor 2 indicator a set of nodes, instead of a single one.

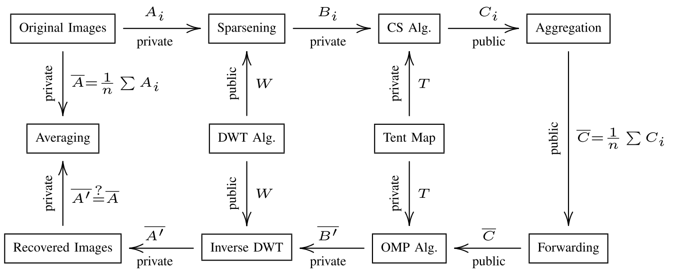

Fig. 3. Proposed CS scheme.

2) *Phase 2:* Sensor 2 chooses an orthogonal matrix W and converts A_i to a sparse matrix $B_i = WA_iW^\tau$ for $i = 1, \ldots, n$, where $W^\tau = W^{-1}$. Then sensor 2 randomly generates a measurement matrix T and computes $C_i = T \cdot B_i$ for $i = 1, \ldots, n$.
3) *Phase 3:* The sink node receives C_i $(i = 1, \ldots, n)$ from sensor 2, calculates an aggregation matrix $C = \sum_{i=1}^n C_i$, and then forwards C to the next hop.
4) *Phase 4:* The final sink node uses the orthogonal matching pursuit (OMP) [40] technique and the measurement matrix T to obtain $B = \sum_{i=1}^n B_i$ from C. Finally, the user computes $A = W'BW$.

The correctness is based on the linear encryption using measurement matrix T, and the encryption has addition homomorphism. That is, we have

$$C = \sum_{i=1}^n C_i = \sum_{i=1}^n (T \cdot B_i) = T \cdot \sum_{i=1}^n B_i = T \cdot B \tag{3}$$

and

$$\begin{aligned} A = W'BW &= W'\left(\sum_{i=1}^n B_i\right)W \\ &= W'\left(\sum_{i=1}^n WA_iW'\right)W = \sum_{i=1}^n A_i. \end{aligned} \tag{4}$$

Note that in the above framework, the public channels are used during the image transmission/forwarding and aggregation processes, while private channels are used during the sampling, compressing, and recovering processes, where the measurement matrix T plays the role of private key. In fact, T can be reconstructed from z_0 and u, i.e., the seed of the chaotic tent map. This suggests the size of the private key is small enough, say 128 bits assuming that each rational number can be represented using 64 bits in implementation. In addition, the discrete wavelet transform (DWT) and its reversion are involved during the sparsening and reconstruction. Both DWT and its reversion can be implemented within the time complexity of $\mathcal{O}(N)$. Another time consuming process is the so-called OMP that can recover an m-sparse signal when the number of measurements is nearly proportional to m [40].

IV. Experiments and Performance Analysis

In this section, we present the performance analysis on the image compression model from six indicators. In the following experiments, the object image is human skull, and three collecting angles are horizontal (hor. for short), coronal (cor. for short), and sagittal (sag. for short).

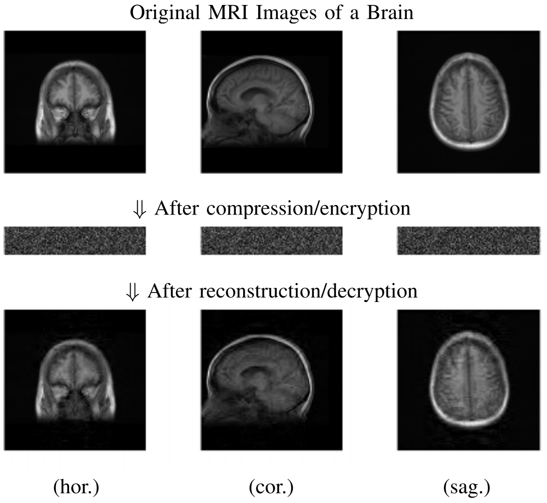
Original MRI Images of a Brain
⇓ After compression/encryption
⇓ After reconstruction/decryption
(hor.)
(cor.)
(sag.)

Fig. 4. Effects of compressed/encrypted sensing.

TABLE I
Runtime of Core Steps

Steps	Runtime (seconds)
DWT	0.1006
Inverse DWT	0.0419
CS	0.0181
OMP	55.4341

A. Overall Effectiveness

The overall effectiveness of CS (as well as encryption) is depicted in Fig. 4. The first row is the original MRI images of a patient's brain (anonymous), scanned horizontally, coronally, and sagittally, respectively, the second row is the corresponding compressed/encrytped images, while the third row is the corresponding recovered images. We can see that on one hand, the compressed images take only 20% of the size of the original images. On the other hand, the encryption results (i.e., the second row) and the recovering results (i.e., the third row) are considerably good.

Our experiments are realized by using MATLAB (version: 2014b), running at a notebook Lenovo ThinkPad with Intel Core i5-4300U CPU@1.9GHz and Window 8 OS. In a typical experiment by setting comparison ratio to 0.2, the runtime of core steps are collected in Table I.

B. PSNR Under Different CR

Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. It is most commonly used to measure the quality of reconstructed images, and the higher is better in general scopes [41]. Considering that many signals have a very wide dynamic range, PSNR (in dB) is usually expressed in logarithmic

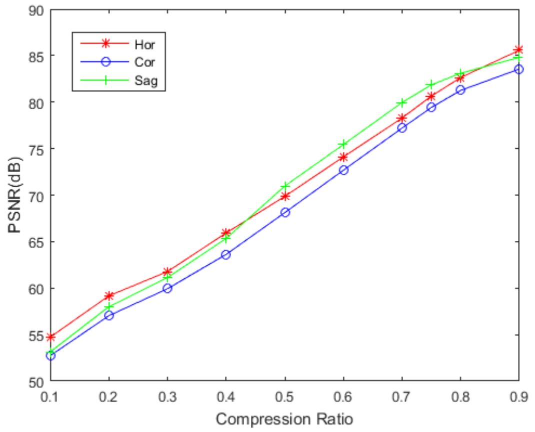

Fig. 5. PSNR versus CR.

decibel scale, and calculated via the mean squared error (MSE). That is,

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right) \quad (5)$$

$$\text{MSE} = \frac{1}{M \cdot N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j) - K(i,j)\right]^2 \quad (6)$$

where M and N are the numbers of pixels of horizontal and vertical coordinates of the image, respectively, while $I(i,j)$ and $K(i,j)$ denote the gray matrices of the original and the reconstructed images, respectively. Here, the constant MAX_I ($= 2^{16} - 1$ in this paper) is the maximum possible pixel value of the image, coming from the fact the used MRI images takes the DICOM format, which consists of three layers and each layer is a 512×512 image with each pixel takes 16-bit gray-scale.

Fig. 5 depicts different PSNR under different compression ratio (CR) for three scanning angles—horizontal, coronal, and sagittal. Here, CR is defined as the ratio between the size of compressed/encrypted and the original images, and the lower is better. We can see that by using the proposed method, PSNR increases almost linearly with the increasing of CR. The experiments indicate that our method has an universal sensing matrix for different images. Furthermore, the compressed sensing reduces significantly transmission energy, also saves transmission bandwidth in the smart health system. Compared to the commonly acceptable criteria of PSNR for wireless transmission quality loss (about 20–25 dB) [42], our method gets a very good balance between PSNR ($\geq$55 dB) and CR ($\geq$0.2).

Note that different from the number theory based encryption scheme, our method cannot preserve the integrity of the original images. Instead, the PSNR metric is merely an *approximation to human perception* of reconstruction quality [41]. In practice, it is an acceptable accuracy criteria for image processing considering that the original images themselves always contain amount of redundance. This is in fact the key basis that we can compress an original image without much loss in human perception of the quality of the reconstructed images.

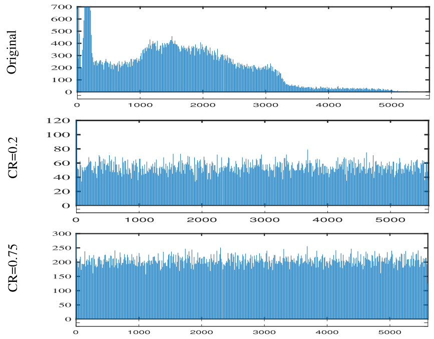

Fig. 6. Histograms of horizontal MRI brain images.

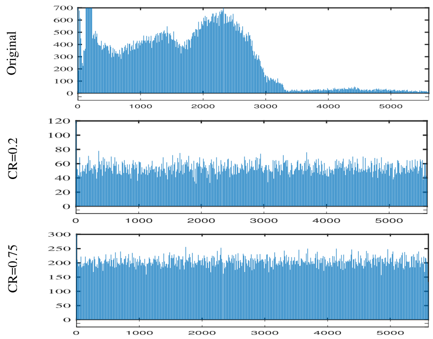

Fig. 7. Histograms of coronal MRI brain images.

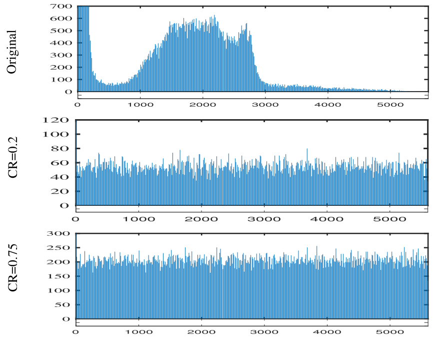

Fig. 8. Histograms of sagittal MRI brain images.

C. Histogram Analysis

An image histogram is a type of graphical representation of the tonal distribution in a digital image that plots the number of pixels for each tonal value. It becomes a very intuitive and popular tool for evaluating the encryption effectiveness for a specific image since a viewer will be able to judge the entire tonal distribution at a glance. In our experiments, three MRI brain images (horizontal, coronal, and sagittal) of size 512×512 (i.e., the first row of columns of Figs. 6–8, respectively) are used, and two different compressing ratio are used: 20% and 75%, respectively. That is, the histograms of encrypted images size are 102×512 (i.e., the second row images of Figs. 6–8, respectively) and 384×512 (i.e., the third row images of Figs. 6–8, respectively). We can see that the gray histograms of the encrypted images are almost uniformly distributed, and the regularities of distribution in the original

TABLE II
CORRELATION

	Horizontal		Vertical		Diagonal	
	original	encryption	original	encryption	original	encryption
Hor	0.9966	0.0078	0.9980	-0.0018	0.9947	0.0002
Cor	0.9953	-0.0034	0.9975	0.0015	0.9931	0.0025
Sag	0.9951	0.0043	0.9961	0.0004	0.9917	0.0047

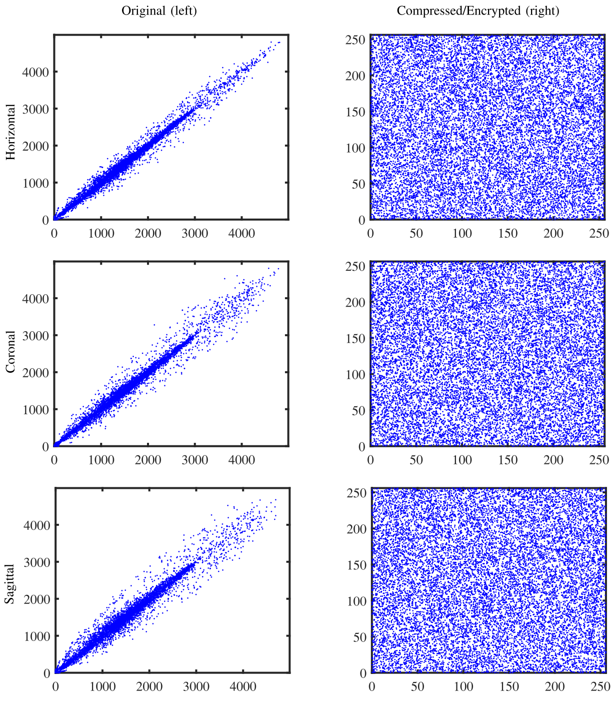

Fig. 9. Adjacent pixels correlation analysis.

images are well covered. Thus, it implies that our scheme has excellent encryption performance of images, and it is infeasible that the attackers are able to extract statistical characters of the plaintext image from ciphertext image, and which can effectively resist statistical analysis attacks.

D. Adjacent Correlation Analysis

Intuitively, a good encryption scheme should maps the distribution of (even adjacent) pixels of the original signals into such a distribution that approximates random and uniform distribution as much as possible. Therefore, adjacent correlation analysis also gives us a view for evaluation the quality of image encryptions.

In our experiments, adjacent pixels correlation analysis is given in Fig. 9 and Table II, where 1600 adjacent pixel pairs from each dataset (i.e., horizontal-skull, coronal-skull, and sagittal-skull) are chosen at random. We can see that the adjacent pixel pairs of the original image are concentratedly distributed in the horizontal, vertical, and diagonal directions, implying that the adjacent pixels correlation of the original image is high. While the adjacent pixels of the encrypted image are dispersed uniformly in the three directions, which implies that the adjacent pixels correlation of the encrypted image is low. These facts further indicate that the proposed scheme can resist the statistical analysis attack effectively.

TABLE III
QUALITATIVE ANALYSIS ON KEY SENSITIVITY

	NPCR(%)	UACI(%)
Hor	74.8200	31.6703
Cor	74.8085	32.2741
Sag	74.8181	31.4970

E. Key Sensitivity Analysis

The number of changing pixel rate (NPCR) and the unified average changed intensity (UACI) are two most common quantities used to evaluate the key sensitivity in image encryption. They are defined respectively as follows [43]:

$$\mathrm{NPCR}(A, B) = \frac{1}{T}\sum_{i,j}\mathrm{diff}\big(A_{i,j}, B_{i,j}\big) \tag{7}$$

$$\mathrm{UACI}(A, B) = \frac{1}{F \cdot T}\sum_{i,j}\big|A_{i,j} - B_{i,j}\big| \tag{8}$$

where T denotes the total number pixels in the ciphertext, F denotes the largest supported pixel value compatible with the ciphertext image format and $\mathrm{diff}(x, y)$ returns 1 if $x \neq y$ and 0 otherwise.

In our experiments with $\mathrm{CR} = 0.2$, we disturb the initial key z_0 slightly by adding 10^{-16}. The resulted metrics of NPCR and UACI of the encrypted images are collected in Table III. We can see that the UACI score is near to the ideal value (33% for 16-bit gray scale), but the NPCR score is a bit far from the ideal value (99.99% for 16-bit gray scale) [43]. This result is undesirable. At present we have not found reasons for this kind of loss in NPCR score and the gap between the NPCR score and the UACI score (note that in calculating the UACI score, we set F to the maximal gray value of pixels in the given two encrypted images, instead of $2^{16} - 1$).

F. Entropy Analysis

The entropies of the original MRI images and the corresponding encrypted images are collected in Table IV, where two sets of simulations corresponding to $\mathrm{CR} = 0.2$ and $\mathrm{CR} = 0.75$, respectively. The entropy of the original images and the entropy of encrypted images are compared in this table. We can see that encrypting significantly enhances the entropy. In particular, considering that the maximal gray

TABLE IV
INFORMATION ENTROPIES

	CR=0.2		CR=0.75
	original	encryption	encryption
Hor	9.4353	12.0917	12.2917
Cor	10.8205	12.7764	12.9726
Sag	8.3548	12.2917	12.4885

value of pixels in the original and encrypted images is about $6000 \in (2^{12}, 2^{13})$ (see the histograms in Figs. 6–8), instead of $2^{16} - 1$, the resulted entropies approximate the optimal.

V. CONCLUSION

In various image-based medical monitoring systems, image compressing, privacy-preserving, and secure data aggregating are three important requirements. In this paper, we propose a novel CS scheme that supports medical image sampling, compressing, encryption, and confidentially homomorphic aggregation simultaneously. On one hand, our proposal has observable advantages in image CR, approximate accuracy, and confidential level. On the other hand, the NPCR score of our method is to be improved and an asymmetric scheme is more desirable over the Internet.

REFERENCES

[1] J. Li, Y. Li, X. Chen, P. P. C. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1206–1216, May 2015.

[2] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: Attack detection using delayed feedback networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 734–743, Feb. 2018.

[3] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Big data toward green applications," *IEEE Syst. J.*, vol. 10, no. 3, pp. 888–900, Sep. 2016.

[4] R. Atat *et al.*, "Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security," *IET Cyber Phys. Syst. Theory Appl.*, vol. 2, no. 1, pp. 49–54, Apr. 2017.

[5] J. Wu *et al.*, "Context-aware networking and communications: Part 1," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 14–15, Jun. 2014.

[6] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 80–88, Feb. 2010.

[7] J. A. Gutierrez *et al.*, "IEEE 802.15.4 a developing standard for low-power low-cost wireless personal area networks," *IEEE Netw.*, vol. 15, no. 5, pp. 12–19, Sep./Oct. 2001.

[8] X. Chang, Z. Ma, M. Lin, Y. Yang, and A. G. Hauptmann, "Feature interaction augmented sparse learning for fast Kinect motion detection," *IEEE Trans. Image Process.*, vol. 26, no. 8, pp. 3911–3920, Aug. 2017.

[9] X. Chang, Z. Ma, Y. Yang, Z. Zeng, and A. G. Hauptmann, "Bi-level semantic representation analysis for multimedia event detection," *IEEE Trans. Cybern.*, vol. 47, no. 5, pp. 1180–1197, May 2017.

[10] J. Xu *et al.*, "Dynamic fully homomorphic encryption-based Merkle tree for lightweight streaming authenticated data structures," *J. Netw. Comput. Appl.*, vol. 107, pp. 113–124, Apr. 2018.

[11] J. Li, Z. Liu, X. Chen, X. Tan, and D. S. Wong, "L-EncDb: A lightweight framework for privacy-preserving data queries in cloud computing," *Knowl. Based Syst.*, vol. 79, pp. 18–26, May 2015.

[12] C. Ding, B. Song, A. A. Morye, J. A. Farrell, and A. K. Roy-Chowdhury, "Collaborative sensing in a distributed PTZ camera network," *IEEE Trans. Image Process.*, vol. 21, no. 7, pp. 3282–3295, Jul. 2012.

[13] D. Xie, H. Peng, L. Li, and Y. Yang, "An efficient privacy-preserving scheme for secure network coding based on compressed sensing," *AEU Int. J. Electron. Commun.*, vol. 79, pp. 33–42, Sep. 2017.

[14] P. Li *et al.*, "Privacy-preserving outsourced classification in cloud computing," *Cluster Comput.*, 2017, doi: 10.1007/s10586-017-0849-9.

[15] L. Wang, J. Li, and H. Ahmad, "Challenges of fully homomorphic encryptions for the Internet of Things," *IEICE Trans. Inf. Syst.*, vol. E99-D, no. 8, pp. 1982–1990, 2016.

[16] W. Chen, H. Lei, and K. Qi, "Lattice-based linearly homomorphic signatures in the standard model," *Theoretical Comput. Sci.*, vol. 634, pp. 47–54, Jun. 2016.

[17] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems—A comparative analysis," in *8th Int. Workshop, DPM 2013/6th Int. Workshop, SETOP 2013*, Egham, U.K., Sep. 2014, pp. 333–349.

[18] E. J. Candès and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.

[19] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[20] A. M. Abdulghani and E. R. Rodriguez-Villegas, "Compressive sensing: From 'compressing while sampling' to 'compressing and securing while sampling,'" in *Proc. 32nd Annu. Int. Conf. IEEE EMBS*, Buenos Aires, Argentina, Aug./Sep. 2010, pp. 1127–1130.

[21] G. Wang, Y. Bresler, and V. Ntziachristos, "Guest editorial compressive sensing for biomedical imaging," *IEEE Trans. Med. Imag.*, vol. 30, no. 5, pp. 1013–1016, May 2011.

[22] J. Li *et al.*, "Secure distributed deduplication systems with improved reliability," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3569–3579, Dec. 2015.

[23] R. Huang and K. Sakurai, "A robust and compression-combined digital image encryption method based on compressive sensing," in *Proc. IEEE 7th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH MSP)*, Dalian, China, Oct. 2011, pp. 105–108.

[24] S. N. George and D. P. Pattathil, "A novel approach for secure compressive sensing of images using multiple chaotic maps," *J. Opt.*, vol. 43, no. 1, pp. 1–17, 2014.

[25] S. N. George and D. P. Pattathil, "A secure LFSR based random measurement matrix for compressive sensing," *Sens. Imag.*, vol. 15, no. 1, pp. 1–29, 2014.

[26] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.*, vol. 62, no. 10, pp. 152–160, 2014.

[27] L. Y. Zhang, K.-W. Wong, Y. Zhang, and Q. Lin, "Joint quantization and diffusion for compressed sensing measurements of natural images," in *Proc. IEEE Int. Symp. Circuits Syst. ISCAS*, Lisbon, Portugal, May 2015, pp. 2744–2747.

[28] Y. Zhang and L. Y. Zhang, "Exploiting random convolution and random subsampling for image encryption and compression," *Electron. Lett.*, vol. 51, no. 20, pp. 1572–1574, Oct. 2015.

[29] H. Liu, D. Xiao, Y. Liu, and Y. Zhang, "Securely compressive sensing using double random phase encoding," *Adv. Mater. Res.*, vol. 126, no. 20, pp. 2663–2670, 2015.

[30] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 71–93, 2014.

[31] Y. Zhang *et al.*, "A block compressive sensing based scalable encryption framework for protecting significant image regions," *Int. J. Bifurcation Chaos*, vol. 26, no. 11, pp. 1–15, 2016.

[32] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. Allerton Conf. Commun. Control Comput.*, 2008, pp. 813–817.

[33] D. Venkatraman and A. Makur, "A compressive sensing approach to object-based surveillance video coding," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 3513–3516.

[34] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression–encryption algorithm based on compressive sensing," *Optik Int. J. Light Electron Opt.*, vol. 125, no. 18, pp. 5075–5080, 2014.

[35] Z. Yang, Y. Xiang, and C. Lu, "Image encryption based on compressed sensing and blind source separation," in *Proc. IEEE Int. Joint Conf. Neural Netw. (IJCNN)*, Beijing, China, Jul. 2014, pp. 1366–1369.

[36] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.

[37] E. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Mar. 2006.

[38] L. Yu, J. P. Barbot, G. Zheng, and H. Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Process. Lett.*, vol. 17, no. 8, pp. 731–734, Aug. 2010.

[39] M. Frunzete, L. Yu, J. P. Barbot, and A. Vlad, "Compressive sensing matrix designed by tent map, for secure data transmission," in *Proc. Signal Process. Algorithms Archit. Arrangements Appl. Conf.*, 2011, pp. 1–6.

[40] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.

[41] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electron. Lett.*, vol. 44, no. 13, pp. 800–801, Jun. 2008.

[42] N. Thomos, N. V. Boulgouris, and M. G. Strintzis, "Optimized transmission of JPEG2000 streams over wireless channels," *IEEE Trans. Image Process.*, vol. 15, no. 1, pp. 54–67, Jan. 2006.

[43] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Selected Areas Telecommun. (JSAT)*, pp. 31–38, Apr. 2011.

Licheng Wang received the B.S. degree in engineering from Northwest Normal University, Lanzhou, China, in 1995, the M.S. degree in mathematics from Nanjing University, Nanjing, China, in 2001, and the Ph.D. degree in engineering from Shanghai Jiao Tong University, Shanghai, China, in 2007.

He is currently an Associate Professor with the Beijing University of Posts and Telecommunications, Beijing, China. His current research interests include cryptography, blockchain, and future Internet architecture.

Lixiang Li received the M.S. degree in circuit and system from Yanshan University, Qinhuangdao, China, in 2003, and the Ph.D. degree in signal and information processing from the Beijing University of Posts and Telecommunications, Beijing, China, in 2006.

She is currently a Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications. Her current research interests include compressive sensing, complex networks, swarm intelligence, and network security.

Jin Li received the B.S. degree in mathematics from Southwest University, Chongqing, China, in 2002, and the Ph.D. degree in information security from Sun Yat-sen University, Guangzhou, China, in 2007.

He is currently a Professor with Guangzhou University, Guangzhou. His current research interests include applied cryptography and security in cloud computing.

Dr. Li was selected as one of Youth Distinguished Scholars of China, Youth Yangzi-River Scholars of China, and New Stars of Science and Technology in Guangdong Province.

Jing Li received the B.S. degree in mathematics from Inner Mongolia Normal University, Hohhot, China, in 2010, the M.S. degree in mathematics from Shanxi Normal University, Xi'an, China, in 2013, and the Ph.D. degree in engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2017.

She is currently an Assistant Professor with Guangzhou University, Guangzhou, China. Her current research interests include cryptography and information security.

Brij B. Gupta received the Ph.D. degree in information and cyber security from the Indian Institute of Technology Roorkee, Roorkee, India.

He is currently an Assistant Professor with the Department of Computer Engineering, National Institute of Technology Kurukshetra, Kurukshetra, India. His current research interests include information security, cyber security, cloud computing, Web security, intrusion detection, and phishing.

Dr. Gupta was a recipient of the Canadian Commonwealth Scholarship Award by the Government of Canada in 2009.

Xia Liu received the M.B. degree in clinical medicine from Binzhou Medical College, Yantai, China, in 1998, the M.S. degree in neuroanatomy from Capital Medical University, Beijing, China, in 2001, and the Ph.D. degree in anatomy from the Chinese University of Hong Kong, Hong Kong, in 2012.

She is currently a Research Associate with Shenzhen Mental Health Institute, Shenzhen, China. Her current research interests include neuroimaging and multimode functional MRI.