An Integration Design of Compression and Encryption for Biomedical Signals

Shaou-Gang Miaou * Shih-Tse Chen Chih-Lung Lin

Department of Electronic Engineering, Chung Yuan Christian University, Chung-Li, Taiwan, 320, ROC

Received 5 October 2002; Accepted 12 November 2002

Abstract

A telemedicine system using communication and information technology to deliver biomedical signals for long-distance medical services has become reality. In either the urgent treatment or ordinary health care, it is necessary to compress the signals for the efficient use of bandwidth. In addition, when compressed biomedical signals or data are delivered over a public channel such as the Internet, their privacy and security would also be an important issue.

The SPIHT (set partitioning in hierarchical trees) is shown recently as an excellent biomedical signal compression method, and the AES (advanced encryption standard) is the state-of-the-art data encryption standard. Data compression and encryption are normally treated as two separate and independent research areas or building blocks in a communication system. However, they are jointly considered in this paper, where we propose a partially encrypting scheme combining SPIHT and AES. In this scheme, compressed SPIHT bit streams are identified based on their importance to signal quality. Then AES is used to encrypt only the important part that can be defined and chosen by a user. The proposed scheme has, therefore, the advantage of encryption scalability. The experiments on electrocardiogram signals and medical images show that the proposed scheme can have significant security protection even only a small portion of compressed data is encrypted, resulting in the considerable saving of processing time.

***Keywords*:** Compression, ECG, Encryption, Medical images, Telemedicine, SPIHT, AES

Introduction

By telemedicine it means the use of telecommunication and information technology for the diagnosis, treatment, and health care of patients at a remote site via wired or wireless communication equipments and high-speed computers. It can also provide the diagnosis service from a group of doctors located at different geographical areas [1]. In many circumstances, a telemedicine system is a must. For example, it is needed in public passenger carriers such as airplane, steamer, train, etc.; or in secluded regions like mountain area, at the sea, etc.; or in a natural disaster scene such as avalanche, earthquake, etc. Either due to the inadequate and imperfect software and hardware for medical services, or the disaster causing the damage of medical facilities, we may still deliver biomedical signals, speech signals, motion pictures and text data by the telemedicine system consisting of mobile communication networks in either case.

Although the broadband network and the third generation cellular system increase the affordable bandwidth, transmitting the great quantity of medical signals in real time may not be always possible. In addition, the data for electronic patient record may become an enormous burden for storage. An effective solution to both bandwidth and storage problem is the use of data compression.

Following the widespread use of computers and the continuous development of communication networks, computers and communication networks are natural mediums for many forms of data exchange in various applications. Generally, we often have a public communication network, where the illegal access of data is always a potential threat. Hence, a lot of network security techniques, including encryption, digital signature and authentication, are proposed. Information security has always been an extremely important issue for national defense, finance, multi-media and medical data. Considering the software and hardware cost, it is still a tough challenge to design a simple and highly effective encryption algorithm.

By convention, data compression and encryption are two separate research areas. Furthermore, compression (source coding) and encryption are two separate and independent coding blocks in a communication system. However, related algorithms have been proposed based on the joint consideration of compression and encryption [2-6]. Cheng and Li gave a short review of this approach [7] and identified many problems associated with current methods. For example, Matias and Shamir's algorithm [2] is simply a transposition

* Corresponding author: Shaou-Gang Miaou
Tel: +886-3-2654609 ; Fax: +886-3-2654699
E-mail: miaou@wavelet.cycu.edu.tw

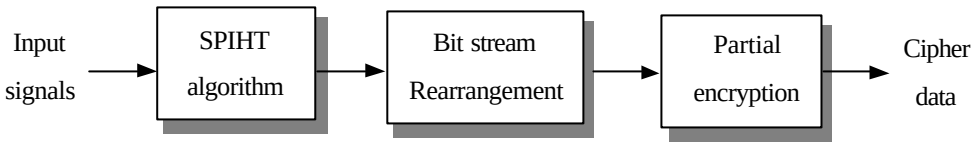


Figure1. A block diagram of the proposed compression/encryption system.

cipher, and therefore, it is easy to suffer from known-plaintext and chosen-plaintext attacks [8]; Jones's algorithm [3] is vulnerable to chosen-plaintext attacks; Bourbakis and Alexopoulos's algorithm [4] also suffers from the chosen-plaintext attack using only one encryption [8]; The algorithm proposed by Chang and Liu [5] is not practical because the encryption key is too long; The algorithm proposed by Liu et al. [6] is approximately twice as slow as the original compression method and the compression performance is also down by 2%.

More recently, Dang and Chau [9] also proposed a combining technique, where discrete wavelet transform (DWT) is used for image compression, and the data encryption standard (DES) is used for encrypting the compressed images. The objective of the approach is to make the data delivery efficient and secure over the network. Unfortunately, it is relatively slow for a general encryption process to satisfy the real-time constraint.

The algorithms described above are either insecure or too computationally intensive. With this consideration, Cheng and Li proposed a partially encrypting algorithm [7], where only significant messages related to pixels or sets in the two highest pyramid levels in a DWT-based encoder are encrypted. The greatest advantage of the approach is to save a great deal of data processing time and to make the real-time processing possible. The very same idea can be applied to the case of transmitting critical biomedical signals, such as electrocardiogram (ECG) and medical images, over the Internet or wireless channels for a telemedicine system. Several questions follow immediately: (1) how to choose a compression method for ECG and medical images; (2) how to choose an encryption method for the compressed data; and (3) how to integrate both methods?

In [10], there is an extensive review of ECG compression algorithms. A short but more recent review can be found in our article [11]. Medical image compression methods are reviewed and discussed in [12-14]. Recently, DWT has been a very popular approach for multimedia data compression. Among all DWT-based methods, the SPIHT [15] proposed by Said and Pearlman has several attractive characteristics, including high compression ratio, low distortion and embedded coding. It works quite well in ECG [11][16-17], speech [18], image [15], medical image [19] and video [20]. It is one of the most excellent state-of-the-art signal compression methods currently available.

As for the data encryption [21-22], DES has been applied extensively to many documents since its official recognition as a standard in 1977. However the computing and processing power of computers is improved so dramatically that DES is no longer considered as a safe encryption standard. With this concern, the National Institute of Standards and Technology (NIST) began to plan for the next generation standard called the advanced encryption standard (AES) in January 1997 [23-24]. The standard was finalized in 2001.

In this paper, we present a coding system consisting of the SPIHT that has excellent compression performance and the AES that is one of the best encryption standards ever proposed. The system takes the advantage of various importance levels of SPIHT bit streams by encrypting only the important bits. A block diagram of the proposed system is shown in Figure 1. First, input signals are compressed by using SPIHT and the resulting bit stream is rearranged according to the visual importance of each bit. Then more important bits are encrypted with higher priority. This partial encryption strategy has the scalability in both processing time and the level of encryption. ECG signals and medical images will be tested for this feasibility study.

In the next section, both SPIHT and AES algorithms are introduced and their integration method is given in Section III. Experimental results and conclusions are given in the last two sections, respectively.

Methods

SPIHT and AES Algorithms

Short Summary of SPIHT

Generally, most of the energy in an image (or ECG) signal is concentrated in the low-frequency region, and the amplitude spectrum of the signal decays with increasing frequency. Furthermore, there is spatial (or temporal) self-similarity among frequency subbands. A spatial (or temporal) orientation tree can be used to define this spatial (or temporal) relationship on the hierarchical pyramid in such a way that each node has either no offspring or four (or two) offspring. All these properties would manifest themselves in the DWT of the signal. The SPIHT is basically an efficient quantization strategy for the resulting coefficients of DWT.

The detail of SPIHT coding can be found in many literatures, say [15] and [16]. Only a short summary is provided here. First, it arranges wavelet coefficients in spatial- (or temporal-) orientation trees. Second, it partitions the coefficients in the tree structure into sets defined by the level of the highest significant bit in a bit-plane representation of their magnitudes. Third, encode and transmit the bits associated with the highest remaining bit planes first.

The coefficient partitioning step is the key to the SPIHT and it consists of two main stages, sorting and refinement. In the sorting pass, a magnitude threshold, 2n, is set, where n is called the level of significance. The subset of coefficients ci in a subband $\Im$ is said to be significant if $\max_{i\in\Im}\{|c_i|\} \geq 2^n$;

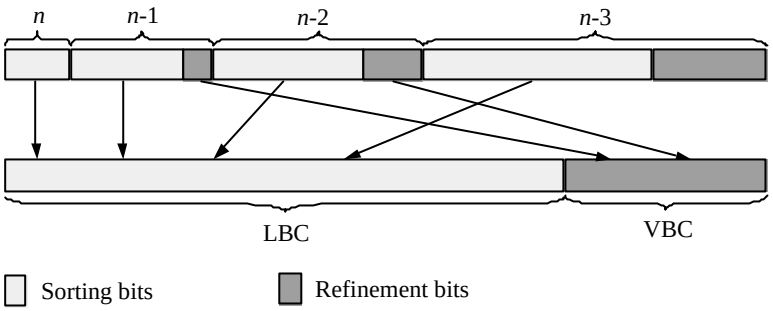


Figure 2. Rearrangement of SPIHT bit stream.

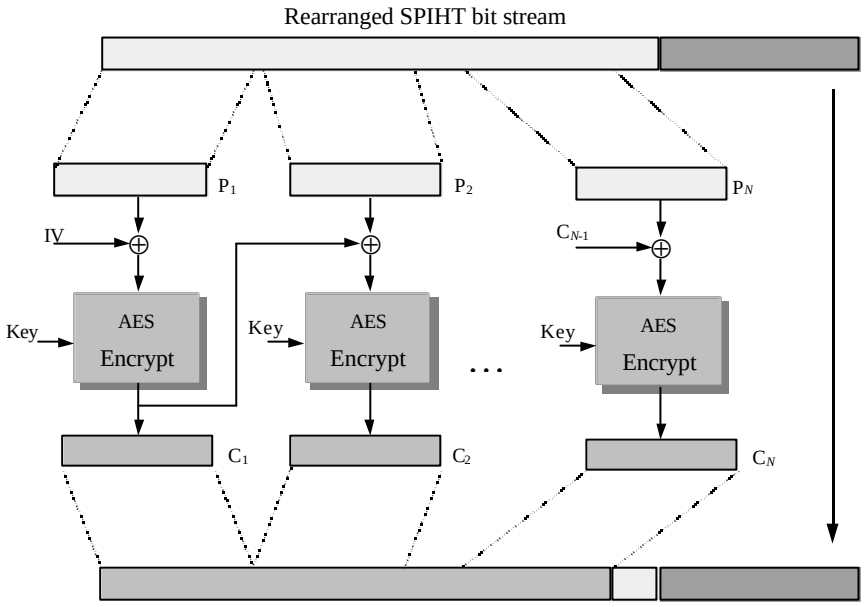


Figure 3. The proposed partial encryption system.

otherwise, it is said to be insignificant. If the subset is significant then it is split further according to the spatial (or temporal) orientation tree until all the significant sets have a single significant element. The SPIHT algorithm tests the significance of the elements in each subset and moves location coordinates of corresponding coefficients to one of three lists: 1) the list of significant coefficients (LSC); 2) the list of insignificant coefficients; 3) the list of insignificant sets. Note that both encoder and decoder will have the same initial lists to begin with. Following each sorting pass, except the first one, is the refinement pass. In the refinement pass, send to the decoder the *n*th most significant bit of the coefficients in the LSC. After the refinement pass, decrease *n* by one, and continue the process until some bit budget or a desired quality level is reached. Following the simple concept of an embedded scalar quantizer, the decoding process is straightforward once the encoded bits for wavelet coefficients are obtained.

Short Summary of AES

In the AES algorithm, the fundamental processing unit is a byte consisting of 8 bits. The input, output or key data are all put into an array whose elements are byte-oriented. The operations in the AES algorithm are represented in terms of "state" which is basically a 4×4 matrix whose element is again a byte. Thus, there are 128 bits in a state. The 4 bytes of each column is defined as a codeword *w*. For the variable-length key state, the number of rows is fixed at 4, whereas the number of column *Nk* could be 4, 6 and 8, corresponding to the key length of 128,196, and 256 bits, respectively.

The AES utilizes the "round" operation to perform encryption and decryption for states. The number of round is defined as *Nr*, and different round numbers are needed for different key lengths. In the beginning of AES encryption procedure, the plain input text is placed in a state. First, the XOR (Exclusive OR) operation is applied between the state and the round key. Then it is encrypted *Nr* rounds. In each round of encryption, it uses all 4 byte-oriented conversions to operate on states. These four conversions are defined as follows: 1) SubBytes: Using a switching table called S-box to perform byte swapping; 2) ShiftRows: For each row in a state array, different units of shifting are performed; 3) MixColumns: Mix columns of the state array; 4) AddRoundKey: The round key is "added" into the state array by performing the XOR operations.

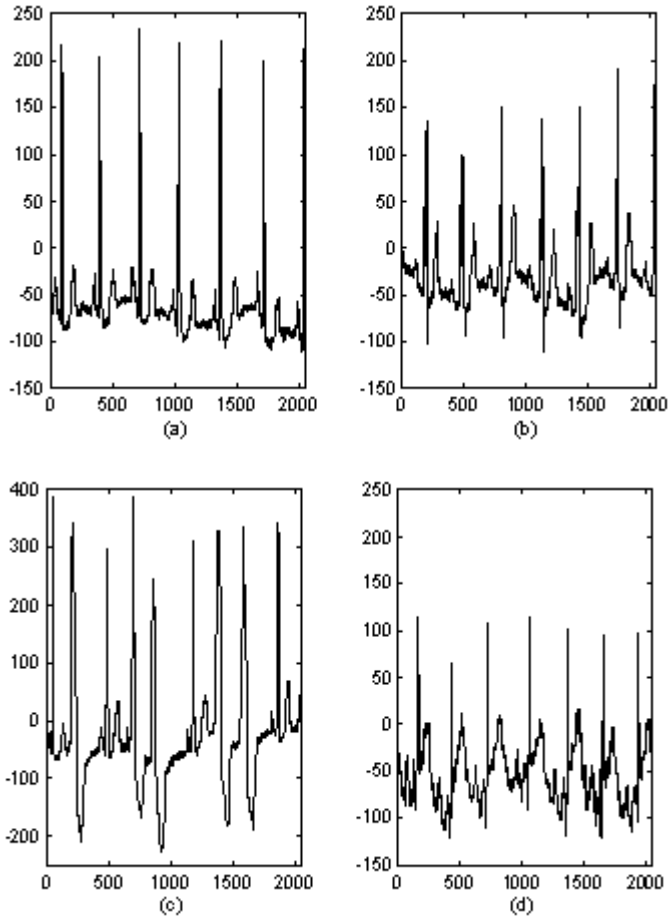


Figure 4. The waveform of the first 2048 samples in each record used in the ECG experiment. (a) Record 101; (b) Record 111; (c) Record 208; (d) Record 228

The proposed algorithm combining SPIHT and AES

Since the SPIHT algorithm has the bit-embedded characteristic, the perceptual importance of the bit stream is roughly decreased from the beginning to the end. For the decoding, losing any important part of bit stream generally means that it is almost impossible to reconstruct the original data. Therefore, encrypting only the important part rather than the entire bit stream may be enough for security protection.

Here, according to the importance of bit stream, it is divided into LBC (location bit class) and VBC (value bit class), where the bits in LBC are generated during the sorting pass of the SPIHT; while the VBC contains the bits generated during the refinement pass. When an error appears in the bit stream of LBC, it will cause the sign errors for important coefficients or wrong coefficient positions in the spatial orientation tree, resulting in serious distortion of reconstructed signals. So the LBC bits can be treated as a bit stream produced from a variable length coder without any look-up-table for decoding and when a critical error happens, it will lead to the phenomenon of error propagation. In this case, the decoder fails completely. When an error takes place in the VBC, it will only affect the accuracy of the reconstructed value of a particular coefficient, and the phenomenon of error propagation does not exist in this case.

Encrypting can be treated as a method that adds known errors to data deliberately, and make it almost impossible to know the information embedded in the original data from only the encrypted cipher text. Taking the characteristics of SPIHT algorithm into consideration, we can rearrange the bit stream at the encoding phase. Our rearrangement here is similar to that in [25], where data are classified for giving different levels of channel error protection. To preserve the order of importance in a bit stream, we place the more important part at the front of bit stream after the rearrangement, as shown in Figure 2.

In Figure 3, it shows a detail flowchart of combining the order-rearranged SPIHT bits with the AES encryption. The rearranged SPIHT bit stream is first divided into N plain text blocks, P_1, P_2, …., P_N. Then the CBC (cipher block chaining) mode [22] along with an IV (initial vector) and a key are used to encrypt these blocks. The encrypted cipher blocks, $C_1, C_2, \ldots, C_N$, together with the remaining plain texts are the final results of encryption. This concludes the process of partial encryption.

If we cannot decode some sorting bits in the LBC successfully, the following bits generally cannot be decoded correctly either. It resembles the error propagation phenomenon for a variable length code. Therefore, we can encrypt only the partial bit stream. A natural question follows

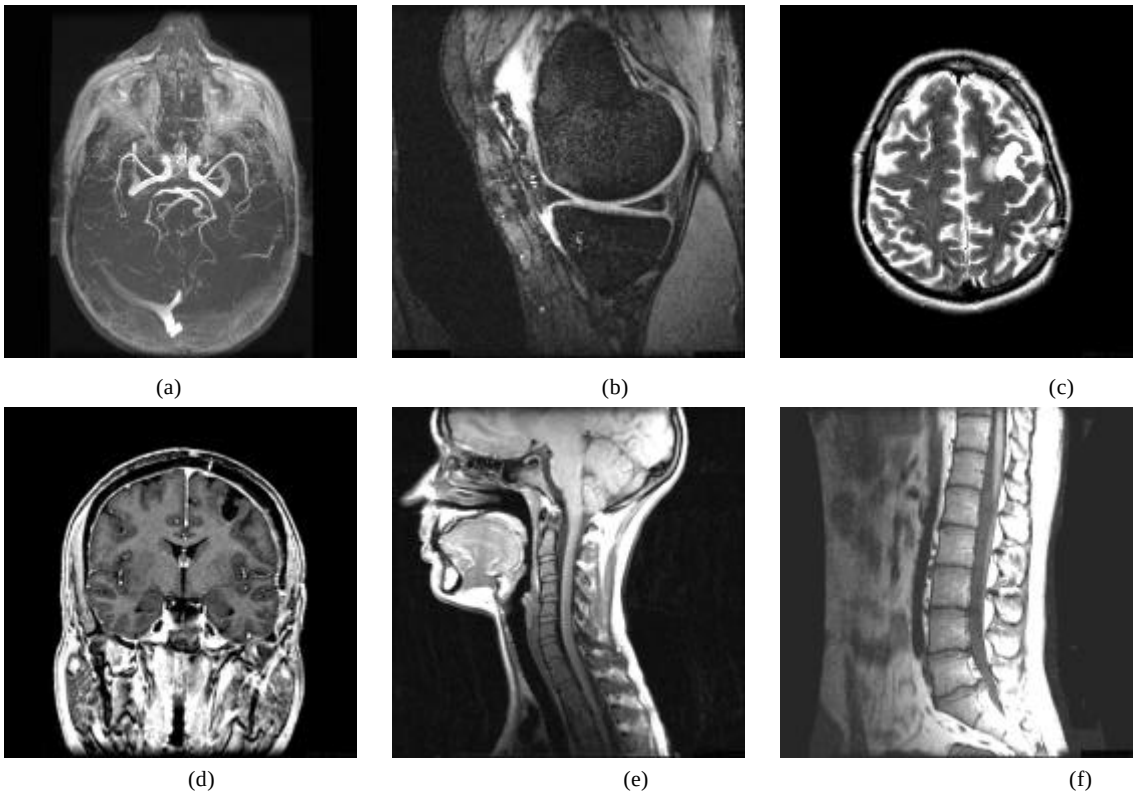


Figure 5. MRI images for the experiment. (a) MRI_1; (b) MRI_2; (c) MRI_3;(d) MRI_4; (e) MRI_5; (f) MRI_6.

would be "how many bits need to be selected for encryption?" This is a tough question that no sound theoretic formulation is available so far to answer it. Here we can only propose a few ideas and principles. Apparently, the length of encrypted bits must be long enough to avoid possible attacks. However, with this lower bound, partial information of the original data may still be revealed if decoding is conducted directly without correct decryption first. If this is the case, the encrypting length can be increased from the lower bound until no meaningful information is shown after the direct decoding.

If the total number of compressed data is x bits and y bits are selected for encryption, then the saving of processing time ΔT can be estimated roughly by

$$\Delta T = \left(1 - \frac{y}{x}\right) T \tag{1}$$

where ΔT is the processing time for the entire compressed data if they are all encrypted. The saving could be very significant if $y << x$.

Experiments and Results

Setup

In the following experiments, all the ECG data records are taken from Lead II of the MIT/BIH arrhythmia database, where four data records with very different waveform morphologies were selected to demonstrate the proposed approach. We illustrate 2048 samples of these four records, i.e., Records 101, 111, 208, and 228, in Figures 4 (a), (b), (c) and (d), respectively. The sampling rate and the resolution are 360 samples/s and 11 bits, respectively. The sample values are all in the range from -1024 to 1023, and the unit of bit rate is bps (bit per second). In the following experiments, 1024 samples/ segment and 6-level DWT are taken as the coding block of the SPHIT. A quality measure such as the percent of root-mean-square difference (PRD) is taken for ECG signals. The PRD is defined as

$$PRD(\%) = \sqrt{\frac{\sum_{i=1}^{L}[x_{org}(i) - x_{rec}(i)]^2}{\sum_{i=1}^{L}[x_{org}(i)]^2}} \times 100\% \tag{2}$$

where x_{org} and x_{rec} denote the original and reconstructed data, respectively, and L is the number of samples within one data segment, which is 1024 in our experiments.

In the experiments of medical image compression and encryption, we take six MRI images, shown in Figure 5, as our test data. All of them are 512×512 8-bit images. In other words, the original bit rate before compression is 8 bpp (bit per pixel). In the following experiments, 5 levels of DWT are applied to each image as the encoding unit of the SPIHT. The peak signal-to-noise ratio (PSNR) is used as the quality criterion for medical images. The PSNR is defined as

$$PSNR(\text{dB}) = 20\log_{10}\frac{I_{\max}}{\sqrt{\frac{1}{IJ}\sum_{i=0}^{I-1}\sum_{j=0}^{J-1}[x_{rec}(i,j) - x_{org}(i,j)]^2}} \tag{3}$$

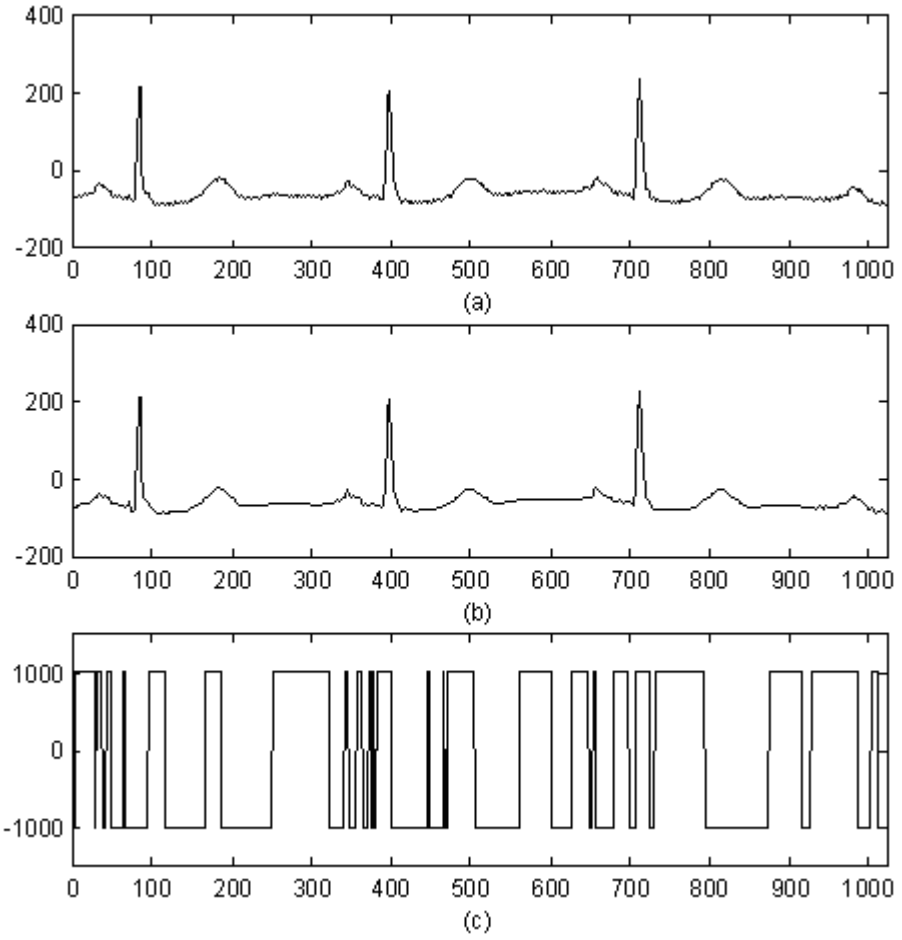


Figure 6. The result of the first segment of Record 101. (a) Original waveform; (b) Decompressed ECG waveform after correct decryption (PRD = 3.33%); (c)Direct decompressed ECG waveform without decryption (PRD = 1549.4%).

Table 1. Key contents and an initial vector.

Key stream	000102030405060708090a0b0c0d0e0f
IV	00000000000000000000000000000000

Table 2. Numerical results for ECG experiments (compression ratio = 8 or bit rate = 495 bps).

Record	Decryption	PRD (%)		
		$N=1$ $\Delta T/T=0.91$	$N=2$ $\Delta T/T=0.82$	$N=3$ $\Delta T/T=0.73$
101	Yes	3.33	3.33	3.33
	No	1549.4	1560.5	1562.5
111	Yes	5.30	5.30	5.30
	No	2328.2	2333.6	2324.6
208	Yes	3.32	3.32	3.32
	No	936.63	930.74	934.94
228	Yes	4.98	4.98	4.98
	No	1638.4	1641.6	1652.7

where $x_{org}(i,j)$ and $x_{rec}(i,j)$ denote the original and reconstructed images, respectively, $I \times J$ is the image size, $I_{\max}=255$ for an 8-bit image, and (i,j) represents the location coordinate pair for a pixel.

We utilize the SPIHT to encode ECG signals and medical images. The compressed data are partially encrypted by AES in the CBC mode with key length = 128 bits. The key contents and an initial vector (IV) in the hexadecimal form for AES are selected arbitrarily and listed in Table 1.

For convenience, the compression ratio is set to 8 for all signals under consideration. In this case, the portion of saving in processing time $\Delta T/T$ can be expressed (according to Eq. (1)) as

$$\frac{\Delta T}{T}=1-\frac{128\times N}{1024\times 11\div 8}\quad (\text{ECG}) \tag{4}$$

$$\frac{\Delta T}{T}=1-\frac{128\times N}{512\times 512\times 8\div 8}\quad (\text{medical images}) \tag{5}$$

where N is the number of encryption blocks as shown in Figure 3.

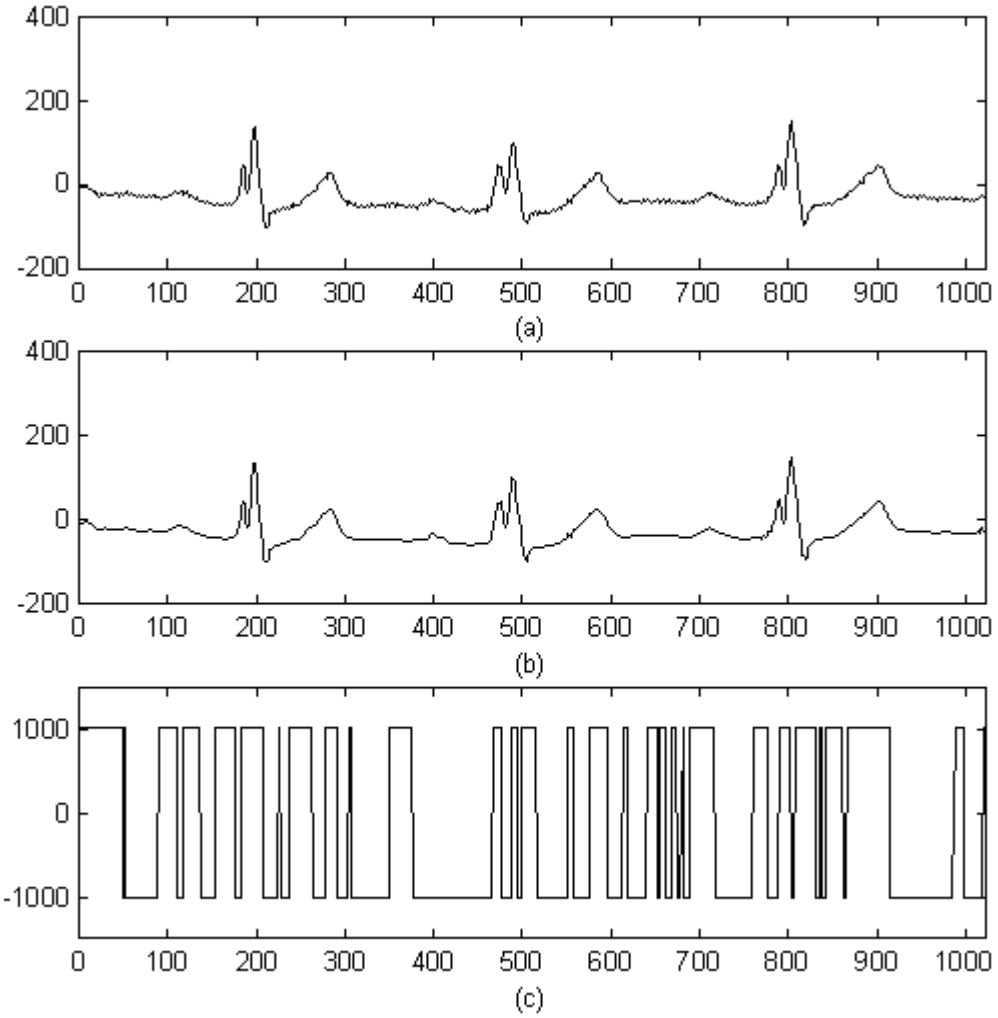
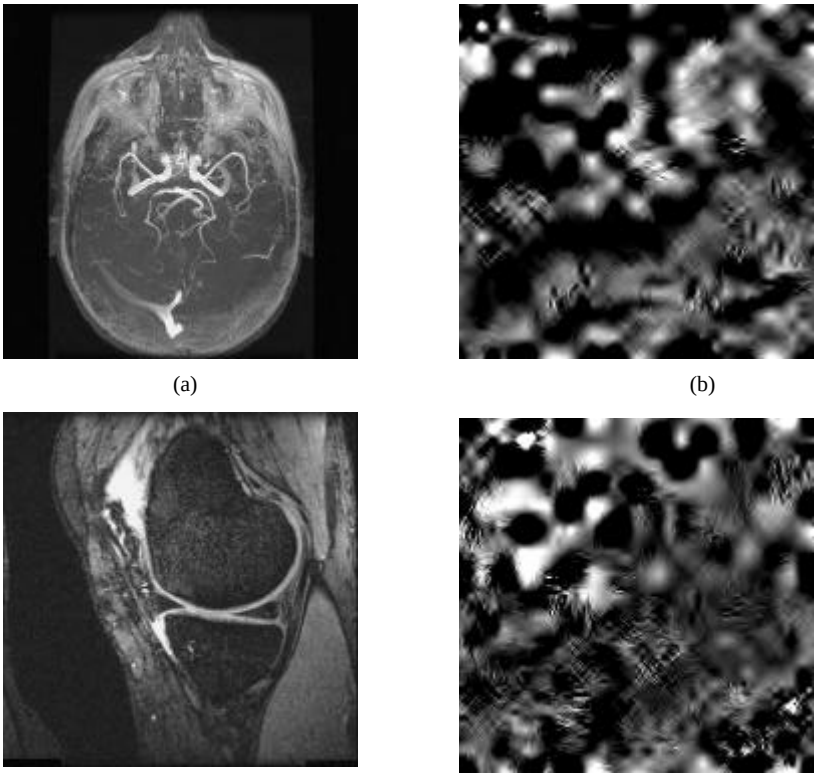


Figure 7. The result of the first segment of Record 111. (a) Original waveform; (b) Decompressed ECG waveform after correct decryption (PRD = 5.30%); (c) Direct decompressed ECG waveform without decryption (PRD = 2328.2%).

Table 3. Numerical results for medical image experiments(compression ratio = 8 or bit rate = 1 bpp).

Image	Decryption	PSNR (dB)		
		$N = 1$ $\Delta T/T = 0.9995$	$N = 2$ $\Delta T/T = 0.9990$	$N = 3$ $\Delta T/T = 0.9985$
MRI_1	Yes	38.19	38.19	38.19
	No	10.02	8.83	8.12
MRI_2	Yes	42.82	42.82	42.82
	No	10.569	8.95	8.60
MRI_3	Yes	42.22	42.22	42.22
	No	8.186	8.13	7.73
MRI_4	Yes	42.23	42.23	42.23
	No	8.0352	7.87	7.06
MRI_5	Yes	44.48	44.48	44.48
	No	7.4464	7.67	7.11
MRI_6	Yes	46.61	46.61	46.61
	No	6.5389	6.06	5.56



(a) (b)

(c) (d)

Figure 8. The MRI results. (a) Decoding with correct decryption first; (b) Direct decoding without decryption of MRI_1; (c) decoding with correct decryption first; (d) Direct decoding without decryption of MRI_2.

ECG Results

The block number N in AES is set to 1 for simplicity. The results of the fist segment of Records 101 and 111 are shown in Figure 6 and Figure 7, respectively. The detailed numerical results for all records are given in Table 2.

Results for Medical Images

In Figure 8, it shows the results of MRI_1 and MRI_2 for the case of $N=1$. In Table 3, it gives the entire numerical results for all medical images.

Discussions

Based on the results on ECG and medical images, we are convinced that the proposed partial encryption system indeed has outstanding secret keeping capability. Even if the SPIHT compressed bit stream is only encrypted partially (128 bits or $N=1$), with no correct decryption, all meaningful information in the original contents is missing. This is because the first few bits in the SPIHT bit stream keep important information regarding the state change of LSC, LIC and LIS, which is essential for correct decoding. If this information is not available immediately, all of reconstructed coefficients and the positions of spatial-orientation trees will be untraceable, and the correct reconstruction of images or ECG is essentially not possible.

A brute-forced attack may require 2^{128} attempts or in this computational order, which is difficult for even the most advanced computers because 2^{128} is a huge number:

$$\begin{aligned} 2^{128} &= (2^{10})^{12} \cdot 2^{8} \\ &= (1024)^{12} \cdot 256 > (10^{3})^{12} \cdot 256 = 2.56 \times 10^{38} \end{aligned} \tag{6}$$

The saving of processing time can be evaluated by the values of $\Delta T/T$ given in Table 2 and Table 3. Based on Eq. (1) and its underlying discussion, the saving obtained here is very significant.

Conclusions

In this paper, we propose an algorithm combining compression and partial encryption to deliver biomedical signals in an efficient and secure manner for telemedicine applications. The experiments on ECG and MRI images clearly demonstrate the feasibility of the algorithm, where great processing time is saved by encrypting only important bits. The decoder will fail miserably if these bits are not decrypted properly. The rearrangement of bit steam of the SPIHT before encrypting and the user selectable scalability of encrypted blocks add additional protection.

The partial encryption approach can save significant processing time in encryption. Thus, we can apply the idea to more speed-demanding data such as volumetric medical images and video sequences for the real-time transmission over public networks.

References

[1] K. Shimizu, "Telemedicine by mobile communication", *IEEE Engineering in Medicine and Biology Magazine*, 18: 32-44, 1999.

[2] Y. Matias and A. Shamir, "A video scrambling technique based on space filling curves", *in Proc. CRYPTO*, 398–417, 1988.

[3] D. Jones, "Applications of splay trees to data compression," *Commun. ACM*, 996–1007, 1988.

[4] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns", *Pattern Recognit.*, 25(6): 567–581, 1992.

[5] H. K.-C. Chang and J.-L. Liu, "A linear quadtree compression scheme for image encryption", *Signal Process. Image Commun.*, 10: 279–290, 1997.

[6] X. Liu, P. G. Farrell, and C. A. Boyd, "Resisting the Bergen-Hogan attack on adaptive arithmetic coding", *in Proc. 6th IMA Int. Conf. Cryptography Coding*, 199–208, 1997.

[7] H. Cheng and X. Li, "Partial encryption of compressed images and videos", *IEEE Trans. Signal Processing*, 48: 2439-2451, 2000.

[8] H. Cheng, "Partial encryption for image and video communication", M.S. thesis, Univ. Alberta, Edmonton, Alta., Canada, 1998.

[9] P. P. Dang and P. M. Chau, "Image encryption for secure internet multimedia applications", *IEEE Trans. on Consumer Electronics*, 46: 395-403, Aug. 2000.

[10] S. Jalaeddine, C. Hutchens, R. Strattan, and W. Coberly, "ECG data compression techniques - a unified approach", *IEEE Trans. Biomed. Eng.*, 37: 329-343, Apr. 1990.

[11] S. G. Miaou, H. L. Yen and C. L. Lin, "Wavelet-Based ECG Compression Using Dynamic Vector Quantization With Tree Codevectors in Single Codebook", *IEEE Trans. Biomed. Eng.*, 49: 671-680, 2002.

[12] S. C. Tai, Y. G. Wu and C. W. Lin, "An adaptive 3-D discrete cosine transform coder for medical image compression", *IEEE Trans. Info. Tech. in Biomed.*, 4: 259-263, Sept. 2000.

[13] Y. G. Wu and S. C. Tai, "Medical image compression by discrete cosine transform spectral similarity strategy", *IEEE Trans. Info. Tech. in Biomed.*, 4: 236-243, Sept. 2001.

[14] Y. G. Wu, "Medical image compression by sampling DCT coefficients", *IEEE Trans. Info. Tech. in Biomed.*, 6: 86-94, 2002.

[15] Said and W. A. Pearlman, "A new, fast and efficient image codec based on set partitioning in hierarchical trees", *IEEE Trans. Circuits Syst. for Video Technol.*, 6: 243-250, 1996.

[16] Z. Lu, D. Y. Kim, and W. A. Pearlman, "Wavelet compression of ECG signals by the set partitioning in hierarchical trees algorithm", *IEEE Trans. Biomed. Eng.*, 47: 849-856, 2000.

[17] S. G. Miaou and C. L. Lin, "A quality-on-demand algorithm for wavelet-based compression of electrocardiogram signals", *IEEE Trans. Biomed. Eng.*, 49: 233-239, 2002.

[18] Z. Lu and W. A. Pearlman, "An efficient, low-complexity audio coder delivering multiple levels of quality for interactive applications", *Proc. IEEE Multimedia Signal Processing*, 529-534, 1998.

[19] Y. Kim and W. A. Pearlman, "Stripe-based SPIHT lossy compression of volumetric medical images for low memory usage and uniform reconstruction quality", *Proc. IEEE Int. Conf. ASSP*, 4: 2031-2034, 2000.

[20] J. Kim, Z. Xiong, and W. A. Pearlman, "Low bit-rate scalable video coding with 3-D set partitioning in hierarchical trees", *IEEE Trans. Circuits Syst. for Video Technol.*, 10: 1374-1387, 2000.

[21] National Bureau of Standards, NBS FIPS PUB 46, Data Encryption Standard, US Department of Commerce, Jan. 1977.

[22] National Bureau of Standards, NBS FIPS PUB 81, DES Modes of Operation, US Department of Commerce, Jan. 1980.

[23] J. Daemen and V. Rijmen, AES Proposal: Rijndael, Document Version 2, March 1999.

[24] http://csrc.nist.gov/encryption/aes/

[25] Alatan, M. Zhao, and A. N. Akansu, "Unequal error protection of SPIHT encoded image bits streams", *IEEE Journal on Selected Areas in Communications*, 18: 814-818, 2000.