IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 19, 2016, accepted December 6, 2016, date of publication March 7, 2017, date of current version April 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2679123

VLSI Implementation of a Cost-Efficient Micro Control Unit With an Asymmetric Encryption for Wireless Body Sensor Networks

SHIH-LUN CHEN, (Member, IEEE), MIN-CHUN TUAN, HO-YIN LEE, AND TING-LAN LIN, (Member, IEEE)

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

Corresponding author: S.-L. Chen (chrischen@cycu.edu.tw)

This work was supported in part by the Ministry of Science and Technology, R.O.C., under Grant MOST-106-2119-M-033-001, Grant MOST-105-2221-E-033-059, Grant 105-2622-E-033-001-CC2, Grant MOST-104-2221-E-033-042, Grant MOST-104-2218-E-033-009, and Grant MOST-104-2622-E-033-007-CC2, and in part by the National Chip Implementation Center, Taiwan.

ABSTRACT This paper presents a very large-scale integration (VLSI) circuit design of a micro control unit (MCU) for wireless body sensor networks (WBSNs) in cost-intention. The proposed MCU design consists of an asynchronous interface, a multisensor controller, a register bank, a hardware-shared filter, a lossless compressor, an encryption encoder, an error correct coding (ECC) circuit, a universal asynchronous receiver/transmitter interface, a power management, and a QRS complex detector. A hardware-sharing technique was added to reduce the silicon area of a hardware-shared filter and provided functions in terms of high-pass, low-pass, and band-pass filters according to the uses of various body signals. The QRS complex detector was designed for calculating QRS information of the ECG signals. In addition, the QRS information is helpful to obtain the heart beats. The lossless compressor consists of an adaptive trending predictor and an extensible hybrid entropy encoder, which provides various methods to compress the different characteristics of body signals adaptively. Furthermore, an encryption encoder based on an asymmetric cryptography technique was designed to protect the private physical information during wireless transmission. The proposed MCU design in this paper contained 7.61k gate counts and consumed 1.33 mW when operating at 200 MHz by using a 90-nm CMOS process. Compared with previous designs, this paper has the benefits of increasing the average compression rate by over 12% in ECG signal, providing body signals analysis, and enhancing security of the WBSNs.

INDEX TERMS Wireless sensor network, micro control unit, QRS complex detector, lossless compression, cryptography, ECC, hardware-shared filter, hardware-sharing, very large-scale integration (VLSI).

I. INTRODUCTION

Nowadays, applications of wireless body sensor networks (WBSNs) [1], [2] have become wider and wider. These applications provide an effective solution for sustained monitoring [2], mobile health [3], self-health management [4] and biological analysis in home-care system [5]. In the future trend of development, such as wireless sensor system [6] for analyzing infectious disease nodes and efficiently protecting sensitive personal data in network security [7], etc., the usage of WBSNs technique is improved rapidly. As the demand of light-weight for wearable and portable applications, development of an efficient device to monitor physical signals via the VLSI technique has become a significant trend.

Many high-performance sensors have been proposed for physical signals. Lee *et al.* [8] proposed an efficiency complementary metal-oxide-semiconductor (CMOS) sensor for body temperature detection. The blood pressure can be detected by a magnetoelastic skin curvature sensor proposed in [9]. The pH value can be measured by an ISFET sensor proposed in [10]. A wearable ECG sensor was proposed in [11]. Although these sensors provided efficient devices to capture the various physical signals, the WBSNs suffered from the limitation of wireless transmission bandwidth, computing resource and energy in batteries.

Several studied concerned hardware-oriented architecture for WBSNs have been presented recently. In order to

save more power consumption and keep longer using time, an adaptive power controller [12] and adaptive fuzzy controller [13] designs were proposed for WBSNs. A multi-channel lossless body-signals compressor [14] was presented for portable monitoring systems. Moreover, to be compatible with handling various bio-signals and processing physical signals in WBSNs, a multi-sensor micro control unit (MCU) was developed in [15]. A bio-signal processing technique was used to improve signal quality in medical applications successfully [16]. By using specific mathematical operations [17], [18], the physical signals can be analyzed with different types.

Lossless data compression techniques are useful in biomedical applications because none of information will be lost during the compression and de-compression processes. Most of low-complexity lossless compression algorithms composed a prediction and entropy coding processes. The combinations of the prediction and entropy coding methodologies include a first-order prediction with a Huffman coding [12], a second-order prediction with a two-stage Huffman coding [19], a fuzzy decision prediction with a hybrid entropy coding [20], and a particle swarm optimizer (PSO) prediction with a Huffman region coding [21].

Although the compressors decrease the data of the physical signals, the compressed data are probably lost during wireless transmission. Hence, an error correct coding (ECC) [22] technique was used to decrease transmission error rates. Chen *et .al* [23] proposed a hardware-intention ECC design, which was successfully integrated into a MCU design. In addition, a universal asynchronous receiver/transmitter (UART) interface design was also integrated into the MCU design. A real-time epileptic seizure controller design was integrated into a CMOS System on a chip (SoC) [24]. Above of those, the data transmission suffered from stolen crisis by wireless transmission module, therefore it is necessary to develop an encryption method to protect personal data. Since the physical signals are important private data for people, the security of body signals is very important. Hence, it is an interesting issue to discuss how to protect the information detected by WBSNs. Symmetric encryption coding [25], [26] used a same key to lock or unlock data in wireless sensor networks (WSNs). This method will fail if one of two sides were cracked. Therefore, Thomas *et al.* [27] proposed a flexible architecture and an asymmetric encryption encoding used in a near-field communication (NFC). Asymmetric encryption [28] is suitable in the field of WBSNs due to two keys, a public key and a private key. The public key is only used to encrypt the plaintext and the private key only works when ciphertext needs to be decrypted.

In addition, some information of physical signals are very important for WBSNs such as the QRS points being very important for ECG signals. C. F. Zhang *et al.* [29] presented a novel QRS detector based on a mathematical morphological method to identify the QRS waves within the ECG signals. Although the hardware-oriented studies [12]–[29] mentioned above achieved the purposes of high performance and low cost designs, it is necessary to develop a new MCU design with more functions, higher performance, and high security for WBSNs.

This paper is organized as follows: In Section II, the concept of WBSNs is presented. VLSI architecture of the proposed MCU design is described in Section III. The experimental results and chip design are shown in Section IV. Finally, a brief conclusion is presented.

II. WIRELESS BODY SENSOR NETWORK SYSTEM

Fig. 1 shows the wireless body sensor networks system and the architecture of the wireless sensor nodes. A typical WBSNs is composed of a group of wireless sensor nodes. Each node includes sensors such as physical sensors, image sensors, an analog-to-digital converter (ADC), a micro control unit (MCU), and a wireless transceiver with an antenna. In WBSNs applications, different physical signals, such as electroencephalography (EEG), electrocardiogram (ECG), thermal, and blood pressure (BP), are captured by different sensors. Hence, the MCU needs to process and merge the physical and imaged data and then send these processed and merged data to a 2.4 GHz band communication system for transmission. Because the communication system is composed of a transceiver, the control commands can be transmitted to the MCU in sensor nodes to change the optional selections from central control system. The specified physical signals captured by the sensors were converted to the signals in digital format by an ADC and then transmitted secretly by the communication system.

After receiving by collection points, the received physical signals will be conveyed to the server for further analysis for users. The information of personal data will be transmitted to ciphertext by using cryptography techniques. Finally, the medical expert can decrypt the ciphertext by a decryption algorithm, analyze the recorded data, and be able to timely provide medical service such as telemedicine or medical consultation. The 2.4 GHz band communication system module will be compatible with different sensor nodes for different types of monitoring applications. Furthermore, the applications of wireless sensor nodes are usually used in the indoor/outdoor field. The issue of power consumptions is very important. Thus, efficient and low-power MCU design become very crucial parts in the wireless body sensor networks.

III. ARCHITECTURE OF MICRO CONTROL UNIT

In order to develop a MCU design for wireless body sensor networks, a cost-efficient and power-efficient architecture of MCU had been developed. Fig. 2 shows the architecture of the proposed MCU design. First, the physical data are detected by the four body sensors from human beings and then transformed as digital data by an analog-digital converter (ADC) device. Second, these digital data are processed by the proposed MCU design which consists of an asynchronous interface, a multi-sensor controller, a register bank,

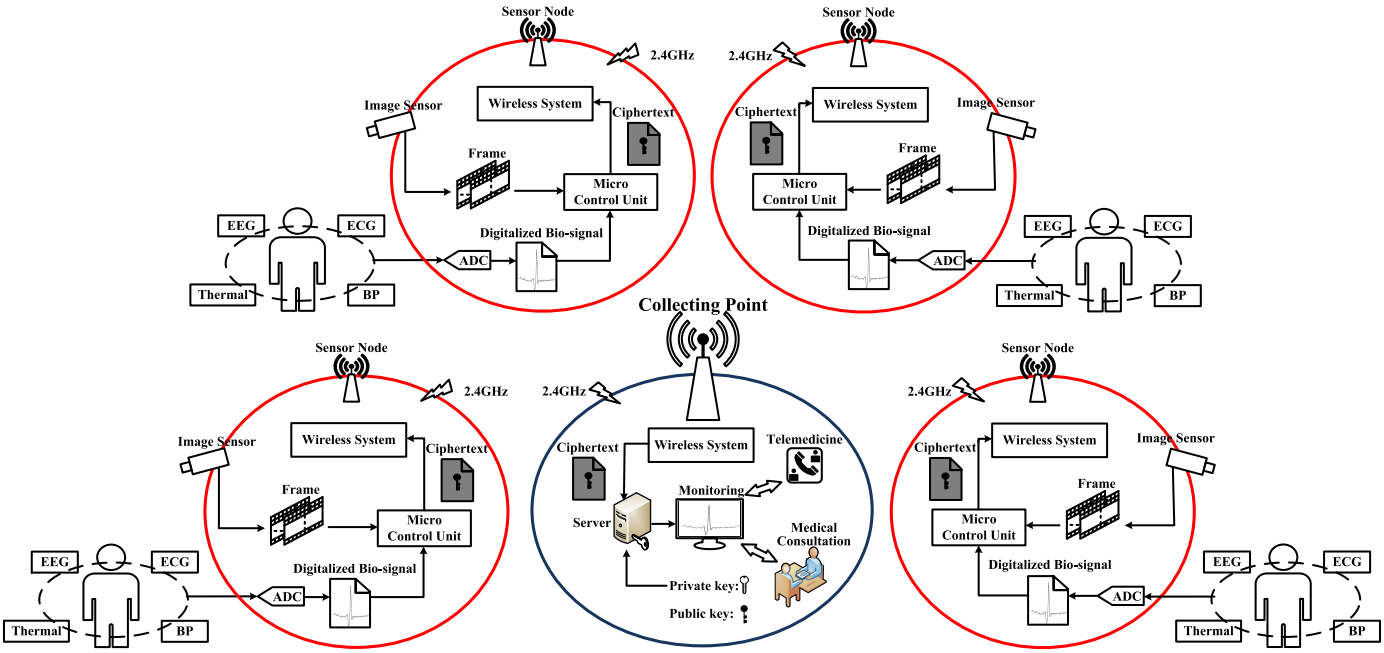

FIGURE 1. WBSNs system and the architecture of the wireless sensor nodes.

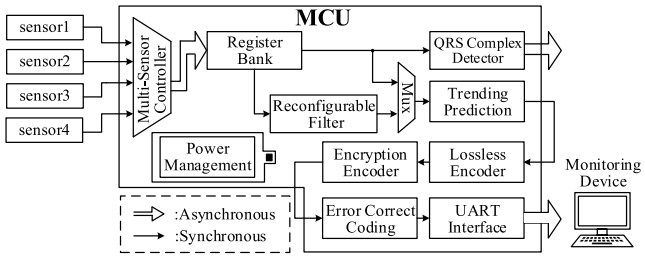

FIGURE 2. VLSI architecture of the proposed micro control unit (MCU).

a hardware-sharing filter, a lossless compressor, an encryption encoder, an error correct coding (ECC), a QRS complex detector, a power management. Finally, the processed digital data will be sent to the UART interface for transmission. All of operations and functions in the proposed MCU design are of low-complexity, which is suitable for development of WBSNs and implementation with a cost-efficient and high performance architecture via the VLSI technique. The details of each circuits are be elaborated in the following.

A. ASYNCHRONOUS INTERFACE

The phases and frequencies of the detected physical signals converted by ADC and UART communication interface are very different with the proposed MCU design. Hence, three asynchronous interfaces [14], [15], [23] were added into MCU design to handle the different phases and frequencies of detected signals. These asynchronous interfaces handle signals communicated between ADC and MCU, those between MCU and those between wireless communication module, and those between MCU and UART interface. Through these asynchronous interfaces, the proposed MCU can receive and transmit signals accurately.

B. MULTI-SENSOR CONTROLLER

The WBSNs contain sensors are used to detect different physical signals from human [14], [15], [23], and the proposed MCU design also supports multi-sensor detection. By generating a control signal to a 4-to-1 multiplexer, the multi-sensor controller can handle four different sensors, such as sensor1, sensor2, sensor3 and sensor4 as shown in Fig. 2. The multi-sensor controller can select one of four signals according to the control signal sent by MCU. Since the multiplexer selects the sensor properly, the MCU can obtain the specified signal for processing successfully. Although more than one sensors are active and sending signals to the MCU simultaneously, the data can still convey sequentially by the multi-sensor controller design. In addition, the multi-sensor controller also controls the signals to store the data to one of four-line register buffers in the register bank of the MCU. Therefore, based on the design of the multi-sensor controller, the proposed MCU design can efficiently prevent data from missing and support four different sensors.

C. REGISTER BANK

In order to process four different signals, a register bank was designed in the proposed MCU. Fig. 3 shows the architecture of the register bank which consists of four-line buffers X_1,

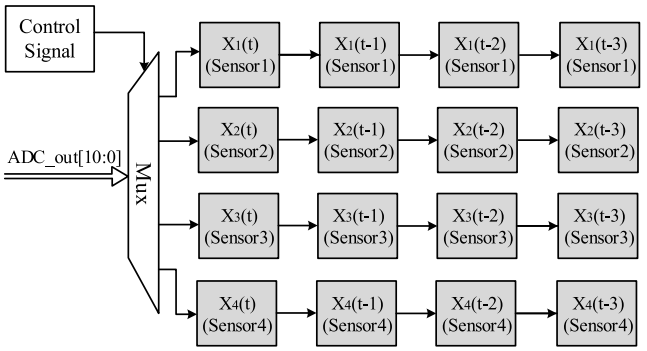

FIGURE 3. Architecture of the register bank.

X_2, X_3, X_4, and one multiplexer. There are 16 shift-registers used to store the four values for each channel. The proposed MCU produces control signal by a finite state machine circuit to classify sensor data. Each channel in the register bank stores four values: the current value X_i (t) and three past values X_i (t-1), X_i (t-2) and X_i (t-3) where "i" is the index of line buffer. Each register can receive only one value of physical signal in each time. The new 11 bits of ADC_OUT value which is obtained by the asynchronous interface, will be stored into the corresponding register based on the control signal of state machine. The proposed register bank design provides important information for the reconfigurable filter and lossless compressor.

D. HARDWARE-SHARED FILTER

The proposed MCU needs to support various physical signal processing. However, the characteristics of each physical signal are distinct. In order to process the signals in different requirements, three types of filters were designed to achieve the abilities of different physical signals filtering: sharpen filter, binomial filter, and average filter. Sharpen filter $G(x)$ uses Gaussian equation [17] to increase the intensity of high frequency parts and filter out low frequency parts of the signal. Binomial filter P(x) can be obtained by Pascal's triangle [18], and the filter can enhance central value and cut off high and low frequency noises. Average filter $A(x)$ uses the same weighting coefficients to calculate average value of the signal stored in register bank. By using the different kinds of filters, the physical signals can be observed apparently. The calculations of sharpen filter $G(x)$, binomial filter $P(x)$, and average filter $A(x)$ are obtained by

$$\mathrm{G}(\mathrm{x}) = \frac{1}{\sqrt{2\pi\sigma}} \mathrm{e}^{\left(\frac{x^2}{2\sigma^2}\right)} \tag{1}$$

$$\mathrm{P}(\mathrm{x}) = (1+\mathrm{x})^{\mathrm{n}} \tag{2}$$

$$\mathrm{A}(\mathrm{x}) = \frac{1}{\mathrm{n}} \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{x_i} \tag{3}$$

where x is the values of the signals, , σ is standard deviation of the Gaussian distribution, n is the number of signals, and i is the index of the signals. Because of the proposed MCU design stored four values of each channel in the register bank, the filtered values of sharpen filter ($G'(x)$), binomial filter ($P'(x)$), and average filter ($A'(x)$) can be calculated by

$$\mathrm{G}'(\mathrm{x}) = \frac{[(-1)\mathrm{X_i}(\mathrm{t}) + 3\mathrm{X_i}(\mathrm{t}-1) + 3\mathrm{X_i}(\mathrm{t}-2) + (-1)\mathrm{X_i}(\mathrm{t}-3)]}{2^2} \tag{4}$$

$$\mathrm{P}'(\mathrm{x}) = \frac{[\mathrm{X_i}(\mathrm{t}) + 3\mathrm{X_i}(\mathrm{t}-1) + 3\mathrm{X_i}(\mathrm{t}-2) + \mathrm{X_i}(\mathrm{t}-3)]}{2^3} \tag{5}$$

$$\mathrm{A}'(\mathrm{x}) = \frac{[\mathrm{X_i}(\mathrm{t}) + \mathrm{X_i}(\mathrm{t}-1) + \mathrm{X_i}(\mathrm{t}-2) + \mathrm{X_i}(\mathrm{t}-3)]}{2^2} \tag{6}$$

The computing resource of sharpen filter $G'(x)$ and binomial filter $P'(x)$ both include five adders and three shifters. In order to decrease the complexity of coefficient calculation, the multiplication of 3 can accomplished by a shifter and an adder. The 2^2 and 2^3 can be calculated by a shifter with different parameters. The computing resource of average filter $A'(x)$ includes 3 adders and 1 shifter. The second column in Table 1 shows the computing resource of the three filters. By this design, the hardware architecture can be implemented by VLSI technique. Although signal filtering is an effective way to process signals appropriately, the silicon cost of each filter will be quite huge when realizing these three filters individually. In [23], a reconfigurable filter combining three filters into one equation was proposed. The principle of reconfigurable filter $R(x)$ simplifies the equations of the sharpen filter, binomial filter, and average filter by

$$\mathrm{R}(\mathrm{x}) = \frac{[\mathrm{k_0X_i}(\mathrm{t}) + \mathrm{k_1X_i}(\mathrm{t}-1) + \mathrm{k_2X_i}(\mathrm{t}-2) + \mathrm{k_3X_i}(\mathrm{t}-3)]}{2^{\mathrm{n}}} \tag{7}$$

where k is the coefficient of corresponding signals. These three types of the filters are suitable for the hardware-intention by using the reconfigurable methodology. Moreover, it was realized by a VLSI architecture as shown in Fig.4(a). The multiplexer is used to select filter parameters by the control signal. The computation of 2^n can be calculated by two shifters.

Through reusing the coefficients in three types of filters, the architecture of the reconfigurable filter combined three functions of filters (a sharpen filter, a binomial filter and an average filter, which are high pass filter, band pass filter and low pass filter respectively) into one module. In order to acquire more detail information in the input signal, the user can select the different types of filters by sending control signals. The sum of computing resource in reconfigurable filter includes 5 adders and 4 shifters as shown in the third column in Table 1. Through this hardware-oriented

TABLE 1. Comparison of computing resource with previous techniques.

Filter	Adder	Shifter	Gate Count
Three Filters (Average, Binomial, Sharpen)	13	7	7.92-K
Reconfigure Filter [23]	5	4	3.24-K
Proposed Hardware-Sharing Reconfigurable Filter	3	3	2.85-K

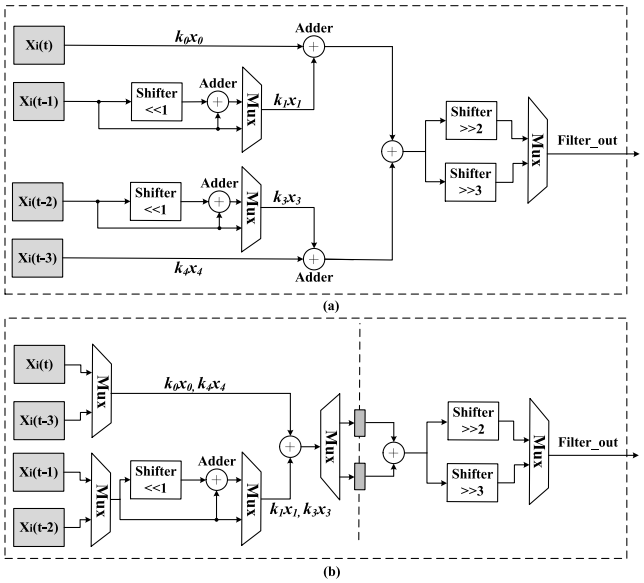

FIGURE 4. Architecture of reconfigurable filter circuit with (a) design in [23], (b) the proposed hardware-shared reconfigurable filter for silicon area reduction.

design, the complexity of the computation can be reduced significantly.

In order to reduce more hardware cost and improve performance of the reconfigurable in this design, a hardware-sharing technique and pipeline design methodology were used. The parameters of filters are stored in two registers which were inserted for pipeline. By hardware-sharing technique, the values of each channel can be computed by the same logic resource in different computing cycles as show in Fig. 4(b). Table 1 lists the comparison of computing resource with previous techniques. It shows that the NAND-equivalent gate counts of three filters (Average, Binomial and Sharpen), reconfigurable filter [23], and the proposed hardware-sharing reconfigurable filter design. These three architectures of filter designs were synthesized by using a Design Compiler in TSMC 0.18 μm CMOS generic logic process technology. The three filters architecture consists of 13 adders and 7 shifters, the gate count is 7.92-K. The reconfigurable methodology includes 5 adders and 4 shifters, which can provide three kinds of filter functions. The proposed hardware-sharing architecture composed of only 3 adders, 3 shifters, and the gate count is 2.85-K gates. The proposed hardware-sharing reconfigurable filter design successfully saved 12% gate counts more than the previous reconfigurable design in Fig. 4(a). Compared with previous designs, the novel architecture achieves lower cost, higher performance and lower complexity than previous designs.

E. LOSSLESS COMPRESSOR

In order to reduce the power consumption caused by the wireless communication and maintain the integrity of physical signals, a lossless compressor including an adaptive trending predictor and a hybrid entropy encoder was created for the

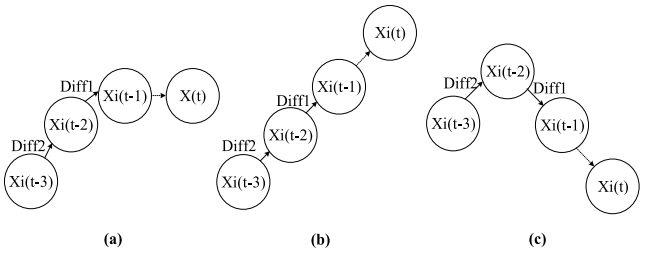

FIGURE 5. The proposed adaptive three-trending-prediction algorithm (a) first-order (b) second-order (c) fluctuation.

WBSNs. To be able to reduce the data redundancy efficiently, an adaptive three-trending-prediction algorithm was proposed. The current value $X_i(t)$ was forecasted by the past three values of $X_i(t\text{-}1)$, $X_i(t\text{-}2)$ and $X_i(t\text{-}3)$. The first-order [12] was used as basic prediction strategy when the signal was in the flat region. The first-order prediction can be obtained by

$$X'_i(t) = X_i(t-1) \tag{8}$$

where $X'_i(t)$ and $X_i(t\text{-}1)$ are the predicted value and the previous value in the register bank respectively. Fig. 5(a) shows the first-order prediction strategy. Since the flat region represents the relationship of current value and previous value are close, the previous value $X_i(t\text{-}1)$ will be selected as predicted current value $X'_i(t)$. Moreover, a second-order prediction [19] method was used as another strategy when the signal was in the linear regions. The second-order prediction can be obtained by

$$X'_i(t) = 2X_i(t-1) - X_i(t-2) \tag{9}$$

where $X'_i(t)$ is the predicted value, $X_i(t\text{-}1)$ is the previous value, and $X_i(t\text{-}2)$ is the second past value in the register bank, respectively. Fig. 5(b) shows the second-order prediction strategy. Since the linear region represents the relationship of current value and the previous values being slope trending, the predicted value will be obtained by the slope relationship. Otherwise, a fluctuation prediction method was used as the final strategy when the signal was in the fluctuation regions. The fluctuation prediction can be obtained by

$$X'_i(t) = X_i(t-1) + \left(\frac{(\text{Diff1} - \text{Diff2})}{4}\right) \tag{10}$$

where $X'_i(t)$ is the predicted value of $X_i(t)$, $X_i(t\text{-}1)$ is the previous value of $X_i(t)$, *Diff1* is the difference between $X(t\text{-}1)$ and $X_i(t\text{-}2)$, and *Diff2* is the difference between $X_i(t\text{-}2)$ and $X_i(t\text{-}3)$. Fig. 5(c) shows the fluctuation prediction strategy. If the absolute values of Diff1 and Diff2 were less than a threshold, the first-order prediction technique *F1* was selected as the prediction methodology. The second-order prediction technique *F2* was selected when the signal was in the linear regions. Otherwise, when the values of Diff1 and Diff2 are of different signs of integers, it was located in the fluctuation region. A modified slope direction *F3* will be selected as a more accurate prediction. By this adaptive trending prediction technique, the accuracies of prediction are

promoted significantly, and the predicted data can be more centralized in the zero-zone for the entropy coding.

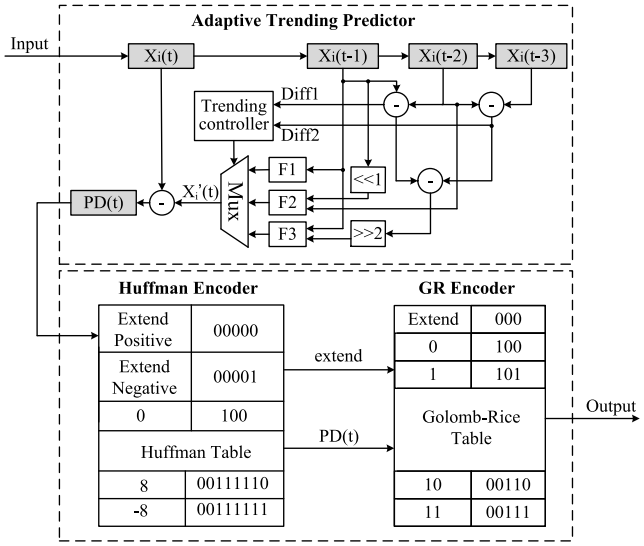

FIGURE 6. Architecture of the proposed lossless compressor.

Fig. 6 shows the architecture of the proposed lossless compressor. It consists of an adaptive trending predictor and an extensible hybrid entropy encoder. The predictor composed of 1 register, 3 subtractors, 1 multiplexer, 3 prediction function generators, and 1 trending controller. The trending controller produced control signals to select a result of $X_i'(t)$ from three prediction function generators *F1*, *F2*, and *F3*. Finally, the prediction difference (*PD(t)*) can be produced by calculating the difference between $X_i(t)$ and $X_i'(t)$.

The extensible hybrid-entropy encoder consists of a modified Huffman and absolute GR encoders. Both of these were variable-length coding methods which can be realized by the architecture of look-up tables. Huffman coding [15] is a classic entropy coding algorithm especially when the probability distribution of target values is centralized. However, the silicon area of a Huffman encoder will be enlarged proportionally to the depth of the Huffman coding tree. Hence, a limited Huffman coding technique was selected as the first stage of the proposed entropy coding methodology, which can avoid the silicon area of the lossless encoder from becoming too huge. Most of the prediction residual values distributed in the range of -8 to 8 were encoded by the limited Huffman coding table as shown in Fig. 8.

In addition, two extending codes, positive and negative extending codes, were added to encode the values beyond the range of the limited Huffman coding table, which successfully improved the performance by removing a sign bit of Golomb-Rice (GR) codes and reduced half silicon area when realized the GR table was realized in the next stage. GR coding is a low-complexity and high-performance entropy coding algorithm which compresses target values according to the relations between the quotient and the remainder. In a traditional GR coding method [14] and [20], it spent double-sized table to handle the sign information of the target values. Since the sign information had been included in the two extending codes of the modified Huffman coding in the previous stage, the proposed GR coding was only to encode the absolute values of the prediction residual values. Since it is unnecessary to handle the sign information, the depth of the proposed GR table, as shown in Fig. 6, can be greatly reduced.

Compared with traditional GR encoder, half of the hardware cost can be saved successfully by the proposed absolute GR coding technique. The value of *PD(t)* will be sent to the GR encoder for encoding only when it is out of the range of the limited Huffman table. Since the proposed modified Huffman encoder was designed with the advantage of positive and negative extending codes to develop absolute model for GR, the range of the absolute GR table was twice of the previous design [14] and [20], costing the same silicon area. The double-range GR table contained twice the ranges of the *PD* distribution, which improved the compression rate of entropy coding efficiently. Finally, the *PD(t)* was encoded by the extensible hybrid-entropy hardware-oriented lossless encoder and then the encoded result $PD'(t)$ be sent out for encryption encoder (EEC).

F. ENCRYPTION ENCODER (EEC)

1) ENCRYPTION ENCODING PROCESSING AND ENCODER DESIGN

In order to prevent the personal information from being cracked and increase the safety for wireless transmission, the encryption encoder is a technique to transfer the plaintext to ciphertext for WBSNs. The principle of the EEC is based on ElGamal cryptography [28] which is a kind of asymmetric encryption coding. ElGamal algorithm is an efficient way to protect the personal information by using two keys: a public key and a private key. In addition, the private key is a confidential parameter and the public key is an open parameter. All of sensor nodes in WBSNs will encrypt the plaintext to protect private data by using public keys and arithmetic modulus. For the attack during the procedure of the wireless transmission, the EEC can avoid personal information from stealing. According to [28], the public key e_2 can be obtained by

$$e_2 = e_1^d \bmod \rho \tag{11}$$

where e_1 and d are the private keys and they will be hidden after calculating by modulo operator (*mod*) of the e_1 to the power of d. The modulo operator can be simplified by

$$e_1^d \div \rho = \alpha \ldots e_2 \tag{12}$$

where the α is a quotient in the division computation and the e_2 is a remainder which is not larger than the divisor ρ. After obtaining public key e_2, the plaintext $PD'(t)$ which is produced by lossless encoder will be encrypted by

$$C_1 = \left(PD'(t) \cdot e_2^{\gamma}\right) \bmod \rho \tag{13}$$

where e_2, γ and ρ are the public keys which are pre-set by the administrator. The ρ is a prime number and the value of ρ is larger than the value of the plaintext. The ciphertext

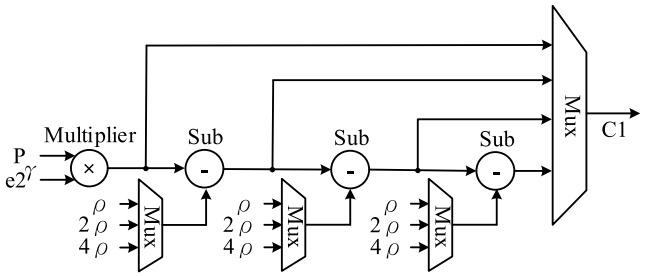

FIGURE 7. Architecture of the proposed encryption encoder.

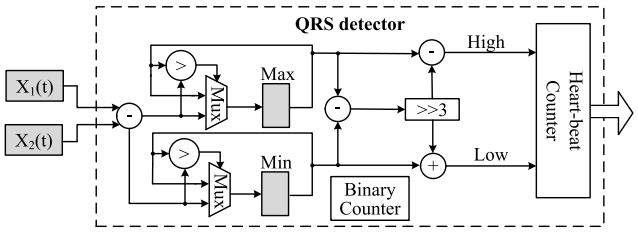

FIGURE 8. Architecture of the proposed QRS complex detector.

C_1 is elaborated and can be generated by equation (12). Fig. 7 shows the architecture of the proposed encryption encoder. It consists of 1 multiplier, 3 subtractors, and 4 multiplexers. The remainder values ciphertext C_1 were calculated by selecting three types of parameters ρ, 2ρ, *and* 4ρ. Finally, the simplified encryption encoder not only provides a low-cost architecture, but also produces better security for the proposed MCU design.

2) DECRYPTION PROCESS

To be able to decrypt the ciphertext which is sent from sensor node, the private key is used. The wireless sensor nodes used public keys to encrypt the personal information, but they cannot use the public key to decrypt the ciphertext. However, the private key set by the administrator is the only one which can decrypt the text. Another private key C_2 can be obtained by

$$\mathrm{C}_2 = \mathrm{e}_1^{\gamma} \bmod \rho \tag{14}$$

where γ and ρ are the public keys. The e_1 and d are private keys. The private key C_2 can be calculated by modulo operator (*mod*) of the e_1 with the power of γ. After obtaining private key C_2, the ciphertext C_1 produced by the proposed MCU design can be decrypted by the plaintext $PD'(t)$ as

$$PD'(t) = \left[\mathrm{C}_1 \cdot \left(\mathrm{C}_2^{\mathrm{d}}\right)^{-1}\right] \bmod \rho \tag{15}$$

G. ERROR CORRECT CODING (ECC)

In order to increase the reliability for wireless transmission, error correct coding (ECC) was added in the proposed MCU design. After the EEC encrypted the signals, the ECC adds additional bits called redundancy codes before the transmission data. The receiver can check whether transmission data are correct or with error before decoding the received data. By generating polynomial function [15], the ECC technique can decrease transmission error.

H. UNIVERSAL ASYNCHRONOUS RECEIVER/TRANSMITTER (UART) INTERFACE

To be able to transmit the bit stream to other devices, a standard communication protocol, called UART interface, was used to communicate between the hardware device and PC. Through FPGA hardware verification procedure [23], the prototype of the proposed WBSNs can be more feasible in the human life. Moreover, the transmission problem such as bit losses, bit errors, unsecure wireless transmission and incompatible problems can be solved by the proposed EEC, ECC, and UART designs.

I. POWER MANAGEMENT (PWM)

Since the MCU device needs to receive and transmit data through asynchronous interfaces and the UART interface, the computing logic elements are the majority of the power consumption in the WBSNs. In order to reduce the power consumption of the MCU device, the power management techniques [12], [15] and [23] were used to intelligently switch between power on and power off for devices of the sensor nodes. For example, when the sensors are available to deliver data or the UART interface is ready for transmission, the PWM will produce control signals to power on the wireless transceiver. All of the circuit modules will work in the same way. Conversely, each function in the wireless sensor node will be turned off to save the power when the tasks of each module is complete. By using the proposed PWM design, the power consumption of WBSNs can be reduced significantly.

J. QRS COMPLEX DETECTOR

In order to achieve the target of multi-function for WBSNs, heart-beats are considered by a QRS complex detector [29] in the proposed MCU design. To obtain the heart-beats information in the real time, the proposed QRS complex detection algorithm detects and records the QRS information by analyzing the critical regions in the ECG signal. For example, the *R* and *S* points usually appear in the maximum (*Max*) and minimum (*Min*) values in the ECG signal, respectively. Hence, the critical regions such as the period of heart-beats can be roughly detected according to information of the detected R and S points. Two thresholds *High* and *Low* are used to determine whether the values enter into the critical regions. The *R* and *S* points are recorded as *Max* and *Min* in order to update the values of *High* and *Low* thresholds, respectively. The *High* threshold can be evaluated by

$$\mathrm{High} = (\mathrm{Max} - (\frac{(\mathrm{Max} - \mathrm{Min})}{2^n}) \tag{16}$$

The *Low* threshold can be evaluated by

$$\mathrm{Low} = (\mathrm{Min} + (\frac{(\mathrm{Max} - \mathrm{Min})}{2^n}) \tag{17}$$

As shown in Fig. 8, the low complexity architecture of the proposed QRS complex detector can be realized and achieved

TABLE 2. Comparison of previous MCU designs with this work.

	[12]	[14]	[15]	[23]	[24]	This work
Compression Rates (MIT-BIH ECG Database)	1.9	2.38	2.26	2.38	-	2.67
Functions	Compression, PWM	Asynchronous, Multi-Sensor Control, Register Bank, Compression, UART Interface	Asynchronous, Multi-Sensor Control, Compression, ECC, PWM	Asynchronous, Multi-Sensor Control, Register Bank, Filter, Compression, ECC, PWM, UART Interface	Register Bank, Memory, FFT, ECC, UART Interface, Seizure Detector	Asynchronous, Multi-Sensor Control, Register Bank, Filter, Compression, EEC, ECC, PWM, UART Interface, QRS Detector
Process (μm)	0.18	0.065	0.13	0.18	0.18	0.09
Frequency (MHz)	100	24	133	133	31.25	200
Gate Counts (-K)	13.4	53.9	2.68	7.67	-	7.61
Power Consumption	150 μW @1MHz	170 μW @24MHz	496 μW @133MHz	1.9 mW @133MHz	2.8 mW @31.25 MHz	15.2 μW @1MHz, 149 μW @24MHz, 190 μW @31.25MHz, 781 μW @133MHz, 1.33 mW @200MHz
Core Area (K-μm^2)	134	58	14	76	13,470	21

heart-beats function by using equations (16) and (17). It consists of 2 registers, 3 subtractors, 1 adder, 2 comparators, 2 multiplexers, 2 shifters, a binary counter and 1 heart-beat counter. Since the measurement of ECG needs two analog sensors to capture signals, these data were stored in channel one and channel two separately. By subtracting with two current values $X_1(t)$ and $X_2(t)$, the proposed QRS detector was designed to record the maximum and minimum values, and calculating the weighting values. Hence, it also included a 13-bit binary counter to set up a period of time for accessing the maximum and minimum registers. The heart-beats can be obtained and sent out by computing the QRS wave position for the ECG signals.

IV. EXPERIMENTAL RESULTS

Table 2 lists the comparisons of the compression rate, functions, process, operating frequency, gate counts, and core area of previous studies [12], [14], [15], [23], [24] and the proposed MCU designs. In order to compare the hardware cost with the previous MCU designs obviously, the gate counts are the equivalent to NAND gate counts. To be able to obtain the performance of the lossless compressor, the compression rates (CR) were used to evaluate the performance of each MCU designs. A MIT-BIH arrhythmia database was selected as library to simulate the compression rates of the previous designs and this work. The average compression rate of whole MIT-BIH Arrhythmia data base in this work is 2.67 which was improved over 12% than those of the previous designs [12], [14], [15], [23] and [24]. The results show that the performance of lossless data encoder is better than previous MCU designs.

This work was also synthesized by using a Design Compiler tool with TSMC 90 nm CMOS generic logic process technology. It contained 7.61-K NAND-equivalent gate counts, and its core area was 20,874 μm^2. Simulation results represent that the proposed MCU design included two functions more than previous designs. The power consumptions in this work were 149 μW and 1.33 mW when operating at 24 MHz and 200 MHz, respectively, which is less than the power consumptions in [12], [14], [15] and [23].

To verify the VLSI architecture of the proposed MCU design, an Altera DE2-115 FPGA development board was used to verify the functions of the proposed hardware design. The utilization of logic elements in this work was 897 and the operating frequency was 50 MHz in the FPGA device. Fig. 9(a) shows the block diagram of the FPGA verification process for this design. First, the physical signals were provided by an Arduino simulator, which is one of open source microcontroller. After receiving the physical signals from the Arduino simulator, the FPGA board including the proposed MCU design received these signals and then processed these signals. Since the verification FPGA board including an UART communication port, the signals processed by the lossless compressor, encryption encoder, and error correct encoder will send to the computer by a UART transmission line. After the computer received the encoded bit stream, the computer can decode the lossless compression, encryption and error correction codes by a decoding software and shows the decoding results on a LCD monitor in the real time as shown in Fig. 9(b). In addition, a logic analyser connected to the FPGA board can show the rates of heart-beats calculated by the QRS complex detector module in the proposed MCU design.

An auto placement and routing tool IC Compiler was used to produce the layout, based on TSMC 90 nm technique, of the proposed MCU design. The layout photograph of the

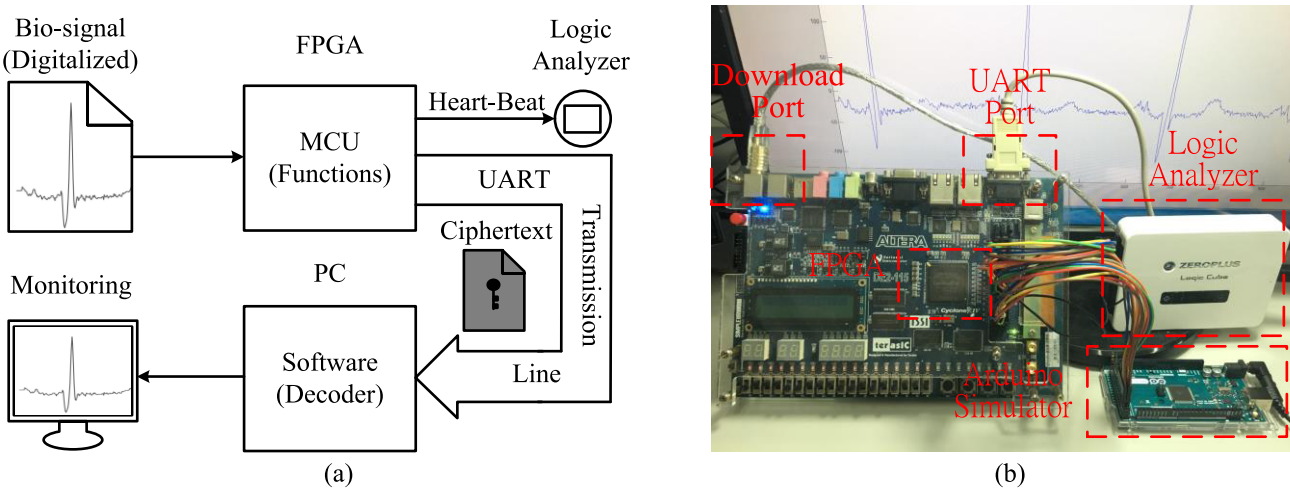

FIGURE 9. FPGA verification of the proposed MCU design. (a) Block diagram of the PFGA verification process, (b) WBSNs demonstration including the Arduino simulator, Altera FPGA board, logic analyzer, and a LCD monitor connected with a computer.

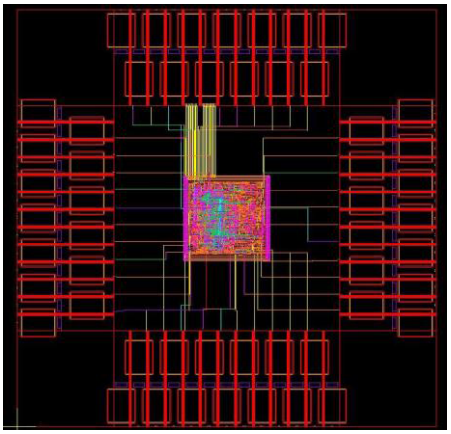

FIGURE 10. Layout photograph of the proposed chip design.

proposed chip design is shown in Fig. 10. The physical core size is 145.32 μm $\times$ 143.64 μm and power consumption is 1.33 mW when operating at 200 MHz. According to Table 2, the proposed MCU design owns two more functions, EEC and QRS detection, than the previous MCU designs [12], [14], [15], [23] and [24]. In addition, the lossless compression rate in this design was much better than previous designs [12], [14], [15], [23] and [24]. Although the gate count and chip area are more than previous design [15], the functions and performances of the proposed design are much better than those of [15]. Compared with the previous studies, this work not only incorporated an additional QRS detector and an encryption encoder, but also had benefits of higher performance, higher security, higher reliability, higher compatibility, more functions, and more flexibility than previous designs.

V. CONCLUSION

In this paper, a VLSI architecture of a cost-efficient and multi-function micro control unit (MCU) design for WBSNs was presented. The novel hardware-sharing filter was design for reducing the chip area and providing three types of filters to obtain more information in physical signals. To reduce the possibilities of misdiagnosis and decrease the transmission power, the lossless compressor which included an adaptive trending predictor and an extensible hybrid entropy encoder was developed. Through adding an asymmetric architecture of encryption encoder (EEC), the personal information can be protected adequately during wireless transmission. Moreover, an additional architecture of QRS complex detector was incorporated into MCU design, which provided more information of physical signals such as heart-beats for the users. As simulation results show, the proposed MCU design was not only completely verified via the FPGA device, but also synthesized by the VLSI technique. Compared with previous designs, this work had benefits of lower cost, higher compression rate, more functions, and higher security than previous studies. It is very suitable for development of WBSNs systems.

REFERENCES

[1] M. Naeem, U. Pareek, D. C. Lee, A. S. Khwaja, and A. Anpalagan, "Wireless resource allocation in next generation healthcare facilities," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1463–1474, Mar. 2015.

[2] H. C. Chuang, C. Y. Shih, C. H. Chou, J. T. Huang, and C. J. Wu, "The development of a blood leakage monitoring system for the applications in hemodialysis therapy," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1515–1522, Mar. 2015.

[3] P. J. F. White, B. W. Podaima, and M. R. Friesen, "Algorithms for smartphone and tablet image analysis for healthcare applications," *IEEE Access*, vol. 2, pp. 831–840, Aug. 2014.

[4] D. Kwon, M. R. Hodkiewicz, J. Fan, T. Shibutani, and M. G. Pecht, "IoT-based prognostics and systems health management for industrial applications," *IEEE Access*, vol. 4, pp. 3659–3670, Jul. 2016.

[5] J.-F. Cheng, J.-C. Chou, T.-P. Sun, S.-K. Hsiung, and H.-L. Kao, "Study on a multi-ions sensing system for monitoring of blood electrolytes with wireless home-care system," *IEEE Sensors J.*, vol. 12, no. 5, pp. 967–977, May 2011.

[6] X. Sun, Z. Lu, X. Zhang, M. Salathé, and G. Cao, "Infectious disease containment based on a wireless sensor system," *IEEE Access*, vol. 4, pp. 1548–1559, Apr. 2016.

[7] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, Oct. 2014.
[8] H.-Y. Lee, S.-L. Chen, and C.-H. Luo, "A CMOS smart thermal sensor for biomedical application," *Inst. Electron., Inf. Commun. Eng.*, vol. E91-C, no. 1, pp. 96–104, Jan. 2008.
[9] E. Kaniusas *et al.*, "Method for continuous nondisturbing monitoring of blood pressure by magnetoelastic skin curvature sensor and ECG," *IEEE Sensors J.*, vol. 6, no. 3, pp. 819–828, Jun. 2006.
[10] P. Rai, S. Jung, T. Ji, and V. K. Varadan, "Drain current centric modality: Instrumentation and evaluation of ISFET for monitoring myocardial ischemia like variations in pH and potassium ion concentration," *IEEE Sensors J.*, vol. 9, no. 12, pp. 1987–1995, Dec. 2009.
[11] E. Nemati, M. J. Deen, and T. Mondal, "A wireless wearable ECG sensor for long-term applications," *IEEE Commun. Mag.*, vol. 50, no. 1, pp. 36–43, Jan. 2012.
[12] S.-L. Chen, H.-Y. Lee, C.-A. Chen, H.-Y. Huang, and C.-H. Luo, "Wireless body sensor network with adaptive low-power design for biometrics and healthcare applications," *IEEE Syst. J.*, vol. 3, no. 4, pp. 398–409, Dec. 2009.
[13] S. L. Chen, "A power-efficient adaptive fuzzy resolution control system for wireless body sensor networks," *IEEE Access*, vol. 3, pp. 743–751, 2015.
[14] E. Chua and W.-C. Fang, "Mixed bio-signal lossless data compressor for portable brain-heart monitoring systems," *IEEE Trans. Consum. Electron.*, vol. 57, no. 1, pp. 267–273, Feb. 2011.
[15] C.-A. Chen, S.-L. Chen, H.-Y. Huang, and C.-H. Luo, "An asynchronous multi-sensor micro control unit for wireless body sensor networks (WBSNs)," *Sensors*, vol. 11, no. 7, pp. 7022–7036, Jul. 2011.
[16] H. Rabbani, R. Nezafat, and S. Gazor, "Wavelet-domain medical image denoising using bivariate Laplacian mixture model," *IEEE Trans. Biomed. Eng.*, vol. 56, no. 12, pp. 2826–2837, Dec. 2009.
[17] J. Tan, D. Baron, and L. Dai, "Wiener filters Gaussian mixture signal estimation with ℓ_∞? -norm error," *IEEE Trans. Inf. Theory*, vol. 30, no. 10, pp. 6626–6635, Oct. 2014.
[18] C. Moraga, R. S. Stankovic, and M. Stankovic, "The Pascal Triangle (1654), the Reed-Muller-Fourier transform (1992), and the discrete pascal transform (2005)," in *Proc. IEEE 46th Int. Symp. Multiple-Valued Logic (ISMVL)*, Jul. 2016, pp. 229–234.
[19] S.-L. Chen and J.-G. Wang, "VLSI implementation of low-power cost-efficient lossless ECG encoder design for wireless healthcare monitoring application," *Electron. Lett.*, vol. 49, no. 2, pp. 91–93, Jan. 2013.
[20] S.-L. Chen, K.-A. Luo, and T.-L. Lin, "Efficient fuzzy-controlled and hybrid entropy coding strategy lossless ECG encoder VLSI design for wireless body sensor networks," *Electron. Lett.*, vol. 49, no. 17, pp. 1058–1060, Aug. 2013.
[21] S.-L. Chen, M.-C. Tuan, T.-K. Chi, and T.-L. Lin, "VLSI architecture of lossless ECG compression design based on fuzzy decision and optimisation method for wearable devices," *Electron. Letters.*, vol. 51, no. 18, pp. 1409–1411, Sep. 2015.
[22] S. C. Krishnan, R. Panigrahy, and S. Parthasarathy, "Error-correcting codes for ternary content addressable memories," *IEEE Trans. Comput.*, vol. 58, no. 2, pp. 275–279, Feb. 2008.
[23] C.-A. Chen, S.-L. Chen, H.-Y. Huang, and C.-H. Luo, "An efficient micro control unit with a reconfigurable filter design for wireless body sensor networks (WBSNs)," *Sensors*, vol. 12, pp. 16211–16227, Nov. 2012.
[24] W.-M. Chen *et al.*, "A fully integrated 8-channel closed-loop neural-prosthetic CMOS SoC for real-time epileptic seizure control," *IEEE J. Solid-State Circuits*, vol. 49, no. 1, pp. 232–247, Jan. 2014.
[25] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 273–289, Jun. 2008.
[26] E. Khan, E. Gabidulin, B. Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks," *IET Wireless Sensor Syst.*, vol. 2, no. 2, pp. 108–114, 2012.
[27] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, and F. Cavaliere, "Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 11, pp. 1965–1974, Nov. 2013.
[28] Arpit and A. Kumar, "Verification of elgamal algorithm cryptographic protocol using linear temporal logic," in *Proc. Int. Conf. Multimedia Technol. (ICMT)*, Aug. 2011, pp. 6662–6665.
[29] C. F. Zhang and T.-W. Bae, "VLSI friendly ECG QRS complex detector for body sensor networks," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 2, no. 1, pp. 52–59, Mar. 2012.

SHIH-LUN CHEN (M'12) received the B.S., M.S., and Ph.D. degrees in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 2002, 2004, and 2011, respectively. He was an Assistant Professor with the Department of Electronic Engineering, Chung Yuan Christian University, Taiwan, from 2011 to 2014, and has been an Associate Professor with the Department of Electronic Engineering since 2014. His current research interests include VLSI chip design, wireless body sensor network, Internet of Things, wearable devices, image processing, data compression, fuzzy logic control, bio-medical signal processing, and reconfigurable architecture.

Dr. Chen received the Outstanding Teaching Award from Chung Yuan Christian University in 2014.

MIN-CHUN TUAN received the B.S. degree and the Dual bachelor's–master's degree from Chung Yuan Christian University, Taiwan, in 2013 and 2014, respectively. He is currently pursuing the Ph.D. degree with the Biomedical/Multimedia IC and System Design Lab, Chung Yuan Christian University. His research fields include image processing, digital chip design, bio-medical signal processing, and FPGA verification.

HO-YIN LEE was born in Hong Kong in 1979. He received the B.S. and Ph.D. degrees in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 2002 and 2007, respectively. He is currently the Technical Director of Shenzhen Hiker Technology Company Ltd. His research fields include medical analog circuit design, medical signal processing, and wireless sensor network.

TING-LAN LIN (S'08–M'11) received the B.S. and M.S. degrees in electronic engineering from Chung Yuan Christian University, Taoyuan, Taiwan, in 2001 and 2003, respectively, and the Ph.D. degree in electrical and computer engineering from the University of California at San Diego, La Jolla, CA, USA, in 2010. In 2008, he was an Intern with the Display System group, Qualcomm, San Diego, CA, USA. Since 2011, he has been an Assistant Professor with the Department of Electronic Engineering, Chung Yuan Christian University, where he has also been an Associate Professor since 2015. His current research interests include video compression, video streaming in lossy networks, optimization of packet prioritization, and perceptual video quality.