INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 4 ISSUE 2 – APRIL 2015 - ISSN: 2349 - 9303

Secure Transmission of Patient Physiological Information in Point of Care System

Mr.K.Prem Kumar[1]
P.G Scholar, Department of CSE
M.Kumarasamy College of Engineering
kam.prem89@gmail.com

Dr.S.Thilagamani[2]
Head of the Department, Department of CSE
M.Kumarasamy College of Engineering
sthilagamani11@gmail.com

Abstract: With an increase in the population of aged people with health issues, nowadays the significance of ECG based remote patient monitoring system as a point of care (PoC) application in the hospitals is getting increased. Patient ECG signal and other physiological information like body temperature, blood pressure, and glucose level, etc., collected by the body sensor networks will be transmitted to the central hospital servers. After processing this information, the system sends the alerts to the doctors if any abnormal condition arises. The major problem with this scenario is, the confidentiality of these information must be potted while the transmission over public channel and storing in the hospital servers. In this paper, an ECG steganography based cryptographic technique is proposed to preserve the confidentiality of the information. The proposed algorithm conceals the encrypted patients' information in the ECG signal without affecting the quality of that signal. It uses the cryptography and ECG steganography techniques to preserve the confidentiality of the patients' information. The effectiveness of the proposed algorithm is evaluated by comparing with the existing algorithms. It is proved that the proposed algorithm is more secure with high processing speed and low distortion of data and host ECG signal.

Index Terms – Point of care system, ECG, cryptography, wavelet, confidentiality, steganography

1 INTRODUCTION

Nowadays the remote health care monitoring systems and Point of care (PoC) applications are more popular as they reduce the medical labor cost and traffic in the medical centers. In emergency cases Point of Care application provides more reliable services by sending the Patient Health Record (PHR) to doctors and necessary actions can be taken in order to save the patients life. Here, the Internet is used as the channel for transmitting the Patient Health Record (PHR) in remote health care monitoring system. In remote health care monitoring system, the body sensor networks are responsible for collecting the ECG signals and the physiological information of the patient. Then, the collected information will be processed by the Personal Digital Assistant (PDA). After all, the processed information will be sent to the central hospital servers through the Internet. Now the doctors can analyze this biomedical information and can take apposite action in case of an emergency using any device from anywhere. As the Internet is used as the communication channel for PHR transmission in remote health care monitoring system, preserving the confidentiality of the patients' health information is a major problem. According to the Health Insurance Portability and Accountability Act (HIPAA), while transmitting the patients health related information through the common channel, it must be sent in a secure way in order to conserve the privacy and confidentiality of the information.

So it is indispensable to develop a security protocol for secure communication and storage of PHR. Several researchers have proposed various techniques for ensuring the confidentiality of the PHR. There are two categories of techniques proposed for the security of the PHR in remote health care monitoring system. First, the techniques use the encryption and decryption algorithms for securing the user data while communication. The encryption algorithms convert actual user data into unknown format that is very hard to understand. The keys used for encryption and decryption of user data play a vital role in the security issues. The notifiable problem with this technique is computational overhead.

Second, the techniques that conceal the sensitive user information inside insensitive information without increasing the size of host information. These techniques are named as steganography techniques. Though it is secure, this steganography technique alone is not sufficient to overcome the problem of secure communication in remote health care monitoring system as stated by HIPAA.

In this paper, a new technique is proposed to guarantee the secure transmission of patient health information collected by body sensor networks. The proposed technique employs both the cryptography and steganography techniques for the secure communication in the remote health care monitoring system. First, the patient physiological information like glucose level, temperature, pressure level, etc., are encrypted using the enhanced encryption algorithm. Then the encrypted information is hidden inside the patient biomedical signal collected by the body sensors. Here the patient ECG signal acts as the host signal in which the patient health information is concealed. Since almost all the health care systems collect ECG signal, the usage of the ECG as host signal is proposed in this paper. Moreover, the ECG signal size is large compared to all other biomedial signals. Therefore it

fits to conceal all other small size information. As a result, the proposed technique guarantees the security of the patient information in the public channel by preventing unauthorized access.

registration request from the patient, SG sends the contract consists of patient's master key (K_m) to the patient. In Encryption phase, the patients information is encrypted with the Session Key (K_s) calculated using K_m, unique part of health information (sn) and identification of the health care

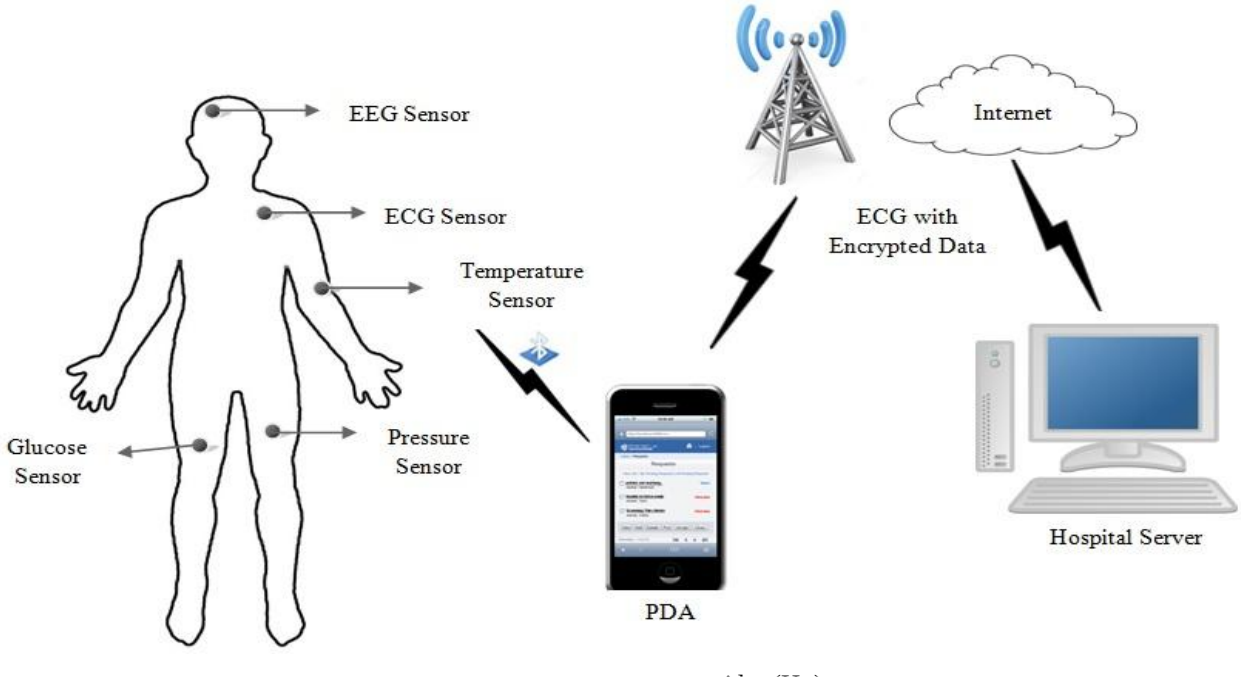


Fig.1. An Point of care (POC) systems where body sensors collect patient's ECG and diagnostics information and watermarking process implemented inside the patient's mobile devices

As the Fig. 1 depicts, in the proposed model, the body sensor nodes will collect all the bio medical information like ECG signal, temperature reading, pressure level, glucose level, etc., and then this information will be sent to the patients PDA device via Bluetooth. Inside the PDA device, the steganography and cryptography techniques will be applied in order to hide the patient secret information inside the ECG signal. Then, the resultant ECG signal is transmitted to the central hospital servers. The patient secret information can be extracted from the host ECG signal only by the authorized persons.

2. RELATED WORK

There are so many approaches proposed to secure the patient confidential data. One approach proposed to secure the data is based on using cryptography technique. Here the patient confidential data is encrypted before transmission. The problem with this approach is computational overhead. As the processing of patient information is done in the PDA, the algorithm used for the encryption and decryption of patient information should not reduce the speed of the PDA device.

Wei-Bin Lee and Chien-Ding Lee [4] proposed an efficient approach for key management in the health care system. The proposed method comprises of three phases named as Registration phase, Encryption phase and Decryption phase. In Registration phase when receiving the

In Decryption phase, the received encrypted patients information is decrypted using the session key (Ks) calculated as same as in encryption phase.The usage of smart card for the key management is proposed here. The notable problem of this scheme is usage of smart card because lots of countries may have problems with smart card adoption. Also the calculation of the session key is highly difficult to implement in PDA devices.

Ilias Maglogiannis et all [6] proposed an architecture for enhancing the location privacy and data encryption in the Patient telemonitoring system (PTS). They proposed the modified Mist architecture for the location privacy and asymmetric encryption algorithm for data encryption. The modification of the Mist architecture for the preservation of location privacy is difficult to understand and implement in real time patient telemonitoring system.

Zheng and Qian [3] proposed a wavelet transform based reversible data hiding. In the proposed method, the B-Spline wavelet transform is applied on the original ECG signal for detecting the QRS complex. Once the R waves are detected, Haar lifting wavelet transform is applied on the original ECG signal. Then, with the help of Index subscripts mapping the non-QRS high frequency wavelet coefficients are selected. Next, the watermarking data are embedded by shifting the selected coefficients 1 bit to the left. Finally, the

reverse Haar lifting wavelet transform applied to construct the ECG signal. Since 1 bit shifting is performed, the notable problem of this approach is low capacity for watermarking. Also this algorithm works on QRS complex of ECG signal which is highly difficult to calculate in abnormal ECG signals. Finally the proposed algorithm does not use any user defined key, thus makes this algorithm more vulnerable for the security attacks.

Golpira and Danyali [2] proposed a wavelet histogram shifting based reversible blind watermarking algorithm for medical images. Here the medical images like MRI image is used as host signal. The proposed algorithm applies 2d-wavelet transform to the MRI images and histogram shifting for watermarking of binary data. This algorithm is only capable of working with the MRI images, thus reduces the capacity for watermarking. Also no encryption of watermarking data is performed. So this algorithm is highly susceptible to security threats.

Kaur et al. [1] proposed quantization based new digital watermarking of ECG data. In the proposed algorithm, each ECG sample is quantized using 10 bits and is divided into segments. The chirp signal is modulated using patient ID, multiplied by a window-dependent factor and added to the ECG signal. Therefore, the final signal consists of 16 bits per sample. The problem of this algorithm is the original size of the host signal gets increased. Since the size of the host signal gets varied after watermarking process, the intruders may be altered about the presence of watermarked data.

3. METHODOLOGY

The proposed technique is enhanced with an authentication process to avert the unauthorized access from extracting the hidden information. The sender side algorithm is designed with four integrated stages as shown in Fig. 2. Whereas the receiver side algorithm consists of as shown in Fig. 3. The proposed algorithm is designed to guarantee the secrete information hiding with minimal distortion of the host ECG signal.

A. Stage 1: Registration

In this phase, the patient has to register his or her details with the point of care system. Here the indenture between the patient and the person who is going to monitor their health condition will be created. This stage crucially focuses on the generation of keys for the encryption and decryption. Along with the personal and health information, a patient has to select two prime numbers for the purpose of key generation. With the support of the selected prime number, the following calculations will be done

$$c = a \times b;\ c > 128 \qquad (1)$$

$$g = (a-1) \times (b-1) \qquad (2)$$

where a and b are the prime numbers selected by the patients while registration. Then the patient must select the encryption key with the following condition

$$\gcd(E, g) = 1\ ;\ 1 < e < c \qquad (3)$$

where gcd represents the greatest common factor of e and g. E represents encryption key. Then the decryption key can be calculated using the following formula

$$D = E^{-1} \pmod{g} \qquad (4)$$

here mod represents the modules operation between E^{-1} and g. The keys for encryption and decryption of patients confidential information are as follows

Encryption key = {E, c}
Decryption key = {D,c}

In completion of registration phase, the key for encrypting and decrypting the information get generated and stored in the user's PDA device.

B. Stage 2: Encryption

The body sensors placed in the patients body calculate the patients physiological information like body temperature, glucose level, pressure level, etc.... These numeric values are transmitted to the patients PDA device that via Bluetooth. Now encryption of the user's information is performed using the following formula

$$P = M^{E} \pmod{c} \qquad (5)$$

Where M represents the numeric value of the patients physiological information. P represents the encrypted value of the patients physiological information.

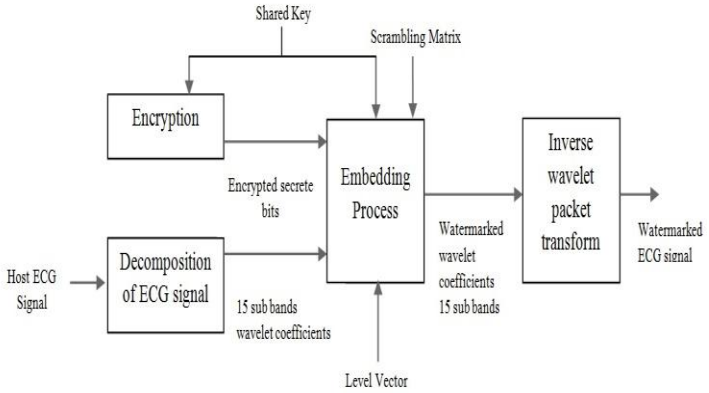


Fig.2. Block diagram of the sender steganography

C: Stage 3: Wavelet Decomposition

The wavelet transform is a process of decomposing the signals over dilated and translated functions called wavelets, which convert the signal into coefficients that represents the frequency of the signal at a given time. The Wavelet transform can be mathematically expressed as follows

$$C(A, B) = \int_{-\infty}^{\infty} f(t)\, \Psi \qquad (6)$$

Where Ψ represents the wavelet function. A and B are positive integers represents transform parameters. C symbolizes the coefficient which is a function of scale and position parameters [9]. The Wavelet transform unite time domain and frequency domain in one transform. Since the ECG signal must be treated in the form of discrete signal, the proposed algorithm uses discrete wavelet transform (DWT). Band filters is used to perform the DWT decomposition by applying wavelet transform. As a result of the decomposition two different signals, one will be associated with the high-frequency components and the other will be related to low-frequency components of the original ECG signal. Here multilevel packet wavelet decomposition is done to decompose the original ECG signal into multiple sub bands of the signals where the embedding of the encrypted user's data is done. The DWT can be defined as follows:

$$W(i,j) = \sum_i \sum_j X(i)\, \Psi_{i,j}(n) \qquad (7)$$

where W(i,j) represents the DWT coefficients , i and j are the scale and shift transform parameters, and $\Psi_{i,j}(n)$ is the wavelet basis time function with finite energy and fast decay. The wavelet function can be defined as follows:

$$\Psi_{i,j}(n) = 2^{-i/2}\, \Psi(2^{-i} n - j) \qquad (8)$$

In this paper, four level wavelet packet decomposition has been applied to the host ECG signal. So that 15 sub bands resulted from this decomposition process. The original ECG signal is divided into two signals in each decomposition that represent high and low frequency components of the original signal. In order to achieve the minimal distortion, different steganography level will be selected for each band. Accordingly, the selected steganography level for bands from 1 to 17 is 5 bits and 6 bits for the other bands [7].

D: Stage 4: Embedding Process

As the Fig.2 portrays, the proposed technique uses the scrambling matrix and level vector for the embedding of the encrypted secrets bits into the decomposed wavelet coefficients. A scrambling operation is done with the help of two parameters. First is the shared key generated in the registration phase. Second is the scrambling matrix with the size 128 x 15. The scrambling matrix is stored inside both the sender and the receiver. So each transmitter and receiver pair has a unique scrambling matrix. The important rule for building the scrambling matrix is there should not any repetition of values in the matrix. The embedding process is done as shown in the Fig.3

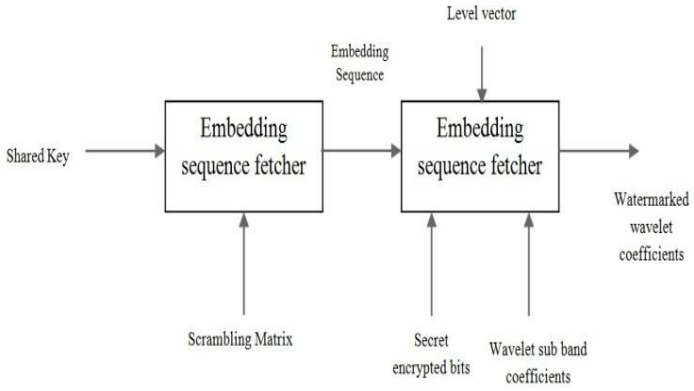
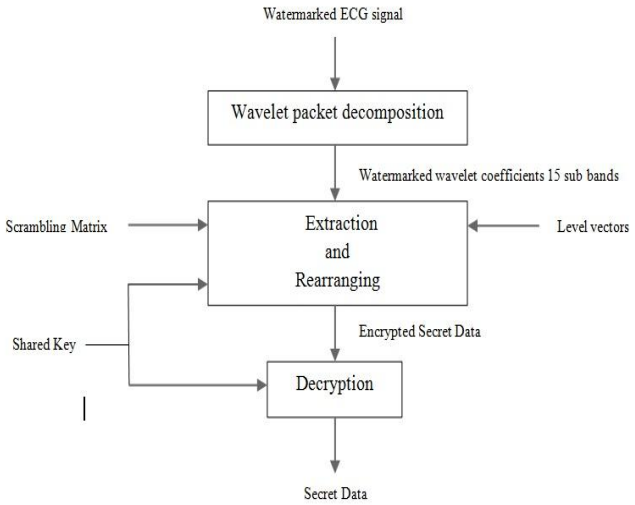


Fig.3. Block diagram of Embedding process

The secret data are embedded in the wavelet coefficients according to the sub band sequence from the fetched row of the scrambling matrix. In the similar way, the steganography level is determined according to the level vector.

E: Stage 5: Inverse wavelet Recomposition

This is the final stage of the sender side. Here the resultant watermarked 15 sub bands are recomposed using inverse wavelet packet Recomposition algorithm. The result of this stage is a watermarked ECG signal. The inverse wavelet Recomposition process converts the wavelet frequency coefficients into time domain signals. The resultant watermarked ECG signal will have minimal distortion and remain diagnosable.



F: Stage 6: Watermark Extraction Process

Fig.4. Block diagram of receiver steganography

This process involves in the extraction of secret information from the watermarked ECG signal. It is necessary to know the shared key, level vector and the scrambling matrix in the receiver side for the extraction of hidden information. The Fig.4 depicts the steps involved in the extraction process.

The watermark extraction process starts with the four-level wavelet packet decomposition to generate the 15 sub bands signals. Then, according to the sequence row fetched from the scrambling matrix the secret bits are extracted using the shared key and scrambling matrix. Finally, the extracted secret bits are decrypted using the same shared key. This stage is performed in the receiver side.

4. RESULTS AND DISCUSSION

As explained, the proposed technique mainly focuses on the following

1. Secure transmission of patients confidential information
2. Minimal distortion
3. High processing speed

In the proposed algorithm, the security of the patients information is based on the three parameters. Any changes in the parameters will restrict the users from accessing the secret information hidden in the ECG signal. So the transmitter and receiver must have the agreement over the following parameters

1. The encryption key
2. Scrambling matrix with the size 128 x 15
3. Steganography Level vector

Even if the encryption key is stolen by the attacker, the hidden information cannot be extracted without knowing the scrambling matrix and steganography level vector. Since the scrambling matrix is stored in the transmitter and receiver device, there is no need of transmission of scrambling matrix. So it is very hard for the third party to get the knowledge about the scrambling matrix. Even the guessing of values of the scrambling matrix is also highly challengeable for the attacker since the size of the matrix is high.

The number of transmitter / receiver pairs with a unique scrambling matrix can be calculated as follows:

$$N = 128! \times 15! \quad (9)$$

The amount of data that can be stored inside the ECG host signal using the proposed algorithm is totally depends on the steganography level vectors. That can be calculated as follows [7]:

$$b = \frac{t \times fs}{15} \times 180 \quad (10)$$

where t is the total signal in seconds, f_s is the sampling frequency and b is the total number of bits stored. As the result of the comparison between the ECG signals showed in the Fig.5, Fig.6 and Fig.7 its clearly proven that after watermarking also the ECG signal remains diagnosable.

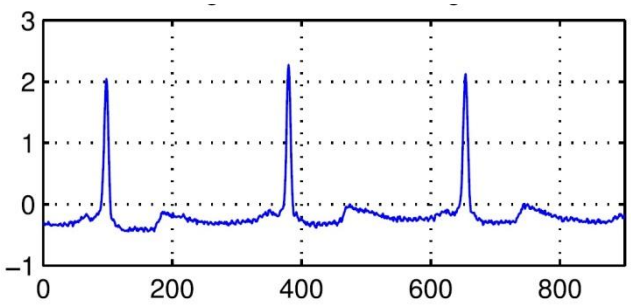


Fig.5. ECG signal before watermarking

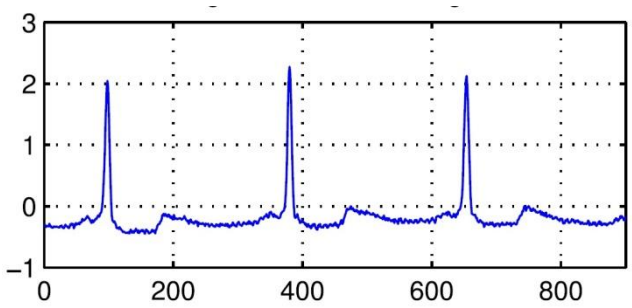


Fig.6. ECG signal after watermarking

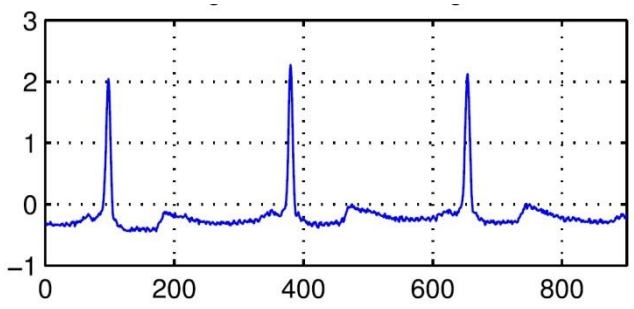


Fig.7. ECG signal after watermark extraction

5. CONCLUSION

In this paper, new ECG steganography based algorithm is proposed to conceal the patients confidential information inside the ECG signal for easy and secure transmission in the point of care system. Here the ECG signals are decomposed into four levels that results 15 sub bands of the frequency coefficients. The ECG signals are decomposed using the discrete wavelet transform concept. The scrambling matrix and the level vectors are used to identify the sub bands for the embedding process. Before embedding, the patients information is encrypted to attain high security. Finally it is proven that the resultant watermarked ECG signal is having the same quality like original ECG signal and the embedded data can be extracted with minimal negligible distortion.

REFERENCES

[1] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, "Digital watermarking of ECG data for secure wireless communication," in *Proc. Int. Conf. Recent Trends Inf. Telecommun. Comput.*, Mar. 2010, pp. 140–144.
[2] H. Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol.*, Dec. 2009, pp. 31–36.
[3] K. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in *Proc. Int. Conf. Comput. Intell. Security*, Dec. 2008, vol. 1, pp. 295–299.
[4] W. Lee and C. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 1, pp. 34–41, Jan. 2008.
[5] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.
[6] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 946–954, Nov. 2009.
[7] Ayman Ibaida *and* Ibrahim Khalil, "Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems," *IEEE Trans.* Biomed., vol. 60, no. 12, Dec 2013
[8] D. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2006.
[9] A. Poularikas, *Transforms and Applications Handbook*. BocaRaton, FL, USA: CRC Press, 2009.