

SPECIAL ISSUE PAPER

A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications

F. Sufi*, F. Han, I. Khalil and J. Hu

School of Computer Science and Information Technology, RMIT University, 123 Latrobe St., Melbourne, VIC-3000, Australia

ABSTRACT

Electrocardiography (ECG) signal is popularly used for diagnosing cardiovascular diseases (CVDs). However, in recent times ECG is being used for identifying person. As ECG signals contain sensitive private health information along with details for person identification, it needs to be encrypted before transmission through public media. Moreover, this encryption must be applied with minimal delay for authenticating CVD patients, as time is critical for saving CVD affected patient's life. Within this paper, we propose the usage of multi-scroll chaos to encrypt ECG packets. ECG packets are being encrypted by the mobile phones using the chaos key by patients' subscribed in tele-cardiology applications. On the other hand, doctors and hospital attendants receive the encrypted ECG packets, which can be decrypted using the same chaos key. Using the techniques described in this paper, end-to-end security can be applied to wireless tele-cardiology application, with minimal processing. Our experimentation with 12 ECG segments shows that with multi-scroll chaos implementation, CVD patients remain completely unidentified, upholding patients' privacy and preventing spoof attacks. Most importantly, the proposed method is 18 times faster than permutation-based ECG encoding, 25 times faster than wavelet-based ECG anonymization techniques and 31 times faster than noise-based ECG obfuscation techniques, establishing the proposed technique as the fastest ECG encryption system according to the literature. Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS

multi-scroll chaos; ECG biometric template protection; CVD patient's privacy; ECG encryption; ECG anonymization technique

*Correspondence

F. Sufi, School of Computer Science and Information Technology, RMIT University, 123 Latrobe St., Melbourne, VIC-3000, Australia.
E-mail: fahim.sufi@student.rmit.edu.au

1. INTRODUCTION

In wireless tele-cardiology applications a patient is often subscribed to a hospital or a monitoring facility for instant cardiovascular disease (CVD) diagnosis, emergency rescue services, event based on site cardiologist attendance, etc. In such a scenario, the patient is attached with portable electrocardiography (ECG) acquisition devices that transmit patient's ECG packets to his mobile phone *via* Bluetooth. Patient's mobile phone then transmits the ECG packets to the hospital through public internet.

Hospital or the monitoring facility, on the other hand, receives the monitored patient's ECG and authenticate the patient, with ECG-based biometric matching. After successful authentication, hospital then knows who this patient is and for what services that patient is subscribed for. Then the patient's ECG is used for diagnosis purposes.

As seen in Figure 1, if the patient's ECG is transmitted without being encrypted (plain text ECG), then it is vulnerable to patient's privacy as well as spoof attack. ECG signal contains the sensitive cardiovascular details of a patient.

Therefore, if these unencrypted ECG segments reach to wrong hands then patient's sensitive health information is compromised, which is against Health Insurance Portability and Accountability Act (HIPAA) regulations [1]. This private health information, if compromised then can be valuable for few organizations, like insurance companies. On the other hand, since ECG can be used for biometric identification, imposter can use the captured ECG segment and use it to gain unauthorized access to secured facilities, such as hospital service.

To protect patient's privacy and possible spoof attack, the ECG segments are required to be encrypted (as it is being done for medical images [2]). In previous studies, we have used permutation cipher [3,4], noised smearing technique [5], and wavelet based [6] technique. However, all of these techniques are computationally expensive for mobile and embedded devices with low computational capacity.

In this paper, we design a multi-scroll chaos cryptosystem for ECG encryption. A chaos system can generate a very long random sequences which can be used to provide many cryptographic keys. This will make it feasible to

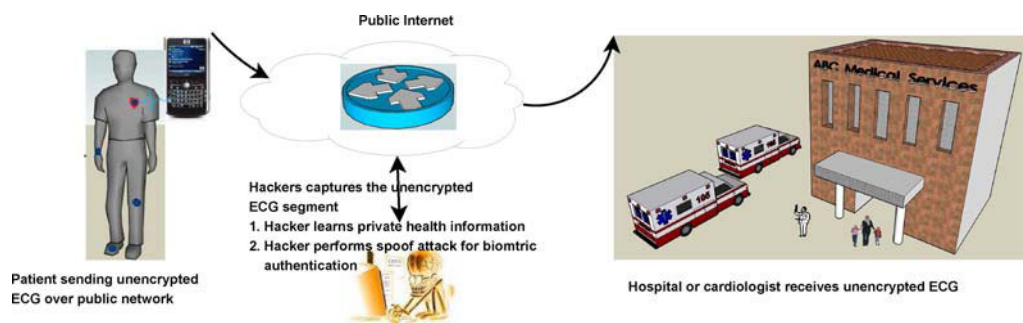


Figure 1. Disadvantages of transmitting unencrypted ECG segments between patient and hospital.

produce a pseudo one-time pad scheme. The Diffie–Hellman protocol has been applied for the distribution of the chaos cryptographic session key. Using 12 publicly available ECG segments, it is shown *via* spectrum analysis that with application of the proposed ECG encryption, the patient's identity remains concealed. Moreover, patient's sensitive health information is protected, upholding HIPAA regulation.

2. BACKGROUND AND RELATED WORKS

Heart is responsible for the maintaining oxygenated blood circulating through out our body, by beating about 100 000 times daily. A typical human heart contains four chambers: two Atria and two Ventricles. The deoxygenated blood first enters the right atrium. The right atrium contracts and pushes the deoxygenated blood to the right ventricle. From the right ventricle the oxygen deficit blood goes to the lungs, where gas exchange process occurs and blood attains oxygen (releases Carbon dioxide). The oxygenated blood then enters the left atria, from where it is redirected to the left ventricle. At the end, the left ventricle forces the blood to the rest of the body. Both the atria contract together and this joint contraction also occurs for the ventricles. This mechanical activity of the heart is spurred by electrical activities of the heart.

ECG is just shows the electrical activity of the hearth. An ECG signal has three major features waves, namely P wave, QRS complex, and T wave (as seen from Figure 2). Atrial contraction results in P wave and ventricular contraction results in QRS complex. T wave, on the other hand, represents ventricular relaxation that occurs after ventricular contraction. Cardiologists have used different features of these feature waves to assess the condition of heart (i.e., CVD Diagnosis). Table I lists some of these features. Earlier ECG biometrics were also based on some of these features [7,8].

As ECG packets contain both patient identifiable features and cardiovascular details of a person, they need to be secured before channelling them through public media.

According to the literature, there are three major types of ECG encryption techniques available: permutation encoding [3,4], wavelet anonymization [6,9], and noise-based obfuscation [5,10].

The permutation encoding technique described in References [3,4] provides substantially higher level of security compared to existing generic encryption algorithms (e.g., AES or DES). According to Reference [4], with a grid of super computers that can compare a trillion trillion trillion (10^{36}) combinations of one ECG segment per second for ECG morphology matching, it will take approximately 9.333×10^{970} years to enumerate all the combinations. Reference [4] also shows how the level of security can be increased even higher by utilizing existing compression and encryption algorithms. In Reference [3], we have shown different level of security strength while using different character encodings (e.g., GSM 03.38, ASCII, UTF-7, UTF-8 etc.).

In References [5,10], noise-based ECG obfuscation techniques was described. These techniques first detects the ECG feature waves (i.e., P wave, QRS complex and T wave), as the features waves are mainly responsible for biometric identification [7,8,11–15] as well as cardiovascular diagnosis [16]. After identification of the feature waves both References [10] and [5] adds distinct noises on top of the feature waves. These specific noises and feature wave template become the key for encryption. The difference in References [10] and [5] is the methodology of feature wave detection.

Lastly, in References [6,9] wavelet-based ECG anonymization techniques were described. Reference [6] used wavelet packet and Reference [9] used discrete wavelet to decompose the ECG into wavelet coefficients. The coefficient corresponding to the lowest frequency component is then intentionally replaced with corrupted values. Then using the coefficients (including the corrupted coefficient) the ECG signal is reconstructed. This reconstructed signal serves the purpose of anonymization. Using the original value of the corrupted coefficient (along with the rest of the coefficients), the anonymized ECG can be decrypted. Therefore, the original value of the corrupted coefficient is the key for encryption/decryption.

Table I. ECG features related to P wave, QRS complex, and T wave.

P wave duration	QRS complex duration	T wave duration
P wave amplitude	QRS complex amplitude	T wave amplitude
P wave onset slope	Q onset slope	T wave onset slope
P wave offset slope	Q offset slope	T wave offset slope
QT interval	R onset slope	P wave direction
RR interval	R offset slope	T wave direction
ST segment	S onset slope	
RR interval	S offset slope	

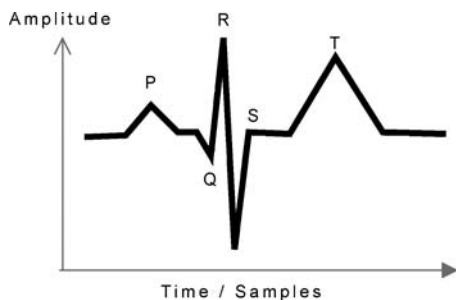


Figure 2. The proposed cardiac diagnosis system.

3. ARCHITECTURE

Unlike existing ECG encryption techniques [3–6], in this paper we use chaos key to encrypt ECG signal. The prime benefit of the architecture presented within this paper over the existing methods is its suitability for computational resource limited mobile (and embedded) devices.

3.1. ECG packet encryption with chaos

As seen in Figure 3 mobile phone receives the ECG signal from the ECG acquisition device and also requests a

chaos key from the chaos generation server. The chaos key is then XORed with the ECG packet, while both of them being the same size (length). After performing the XOR operation between the ECG packet and the chaos key, the resultant is encrypted ECG. Equation (1) represents the original ECG (unencrypted). ψ is the chaos key required to encrypt the unencrypted ECG, $e(n)$. Equation (2) shows the XOR operation for retrieving the encrypted ECG τ .

$$e(n) = x(1), x(2), x(3), \dots, x(N) \tag{1}$$

where, N is the length of the ECG packet.

$$\tau(n) = e(n) \oplus \psi \tag{2}$$

Decryption operation is represented in Equation (3), where the chaos is XORed with the encrypted ECG, τ and the original ECG ($e(n)$) is retrieved.

$$e(n) = \tau(n) \oplus \psi \tag{3}$$

Encrypted ECG does not reveal the patient identifiable characteristics, as well as private health information. Therefore, the encrypted ECG can be freely transmitted over the public internet. Even if the hacker with a malicious intention captures the ECG packet, the patient remains completely anonymized.

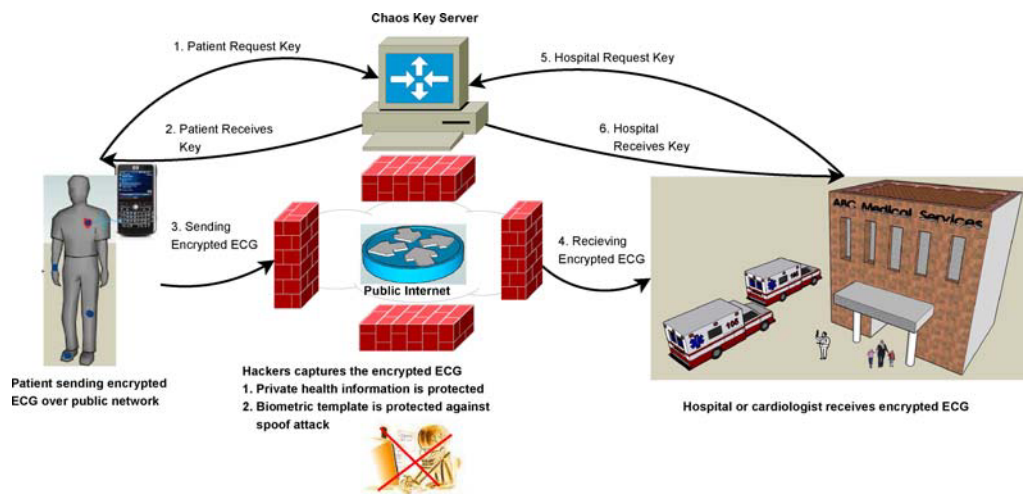


Figure 3. Architecture of the proposed chaos-based ECG encryption system.

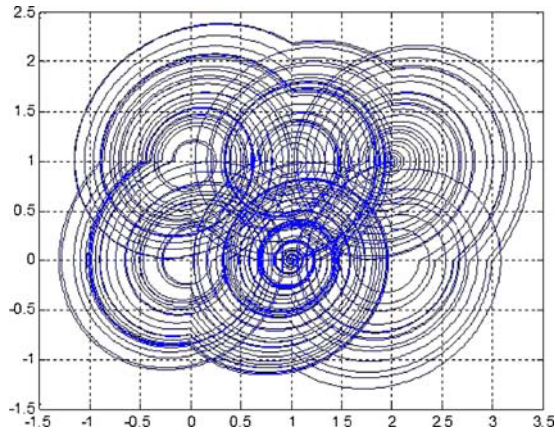


Figure 4. xy projection of a 3×2 -scroll chaos.

When the cardiologist and the hospital receive the encrypted ECG, they need to request the chaos key used for encrypting the ECG. After receiving the same chaos key from the chaos server, it is XORed with the encrypted ECG to decrypt the original ECG.

Therefore, using this architecture a single XOR operation is required to either encrypt or decrypt a single ECG packet. Only XOR operation basically establishes end-to-end security within the link between the patient and doctor (or hospital).

3.2. Random key generation

The chaos key server generates true random binary keys. Chaotic systems are sensitive to initial conditions, and this sensitivity results in long-term unpredictability. True random sequences generated from double-scroll chaotic attractors for cryptographic applications have been proposed and it is indicated that more complex attractors may further improve unpredictability [17,18].

We designed a multi-scroll chaos system (Chaos Key Server of Figure 3) and used it for generating true random sequences for the encryption of large volume of ECG signals. The core theories behind the chaos used is detailed in References [19,20]. Following is the description of our design. With the switching of hysteresis-series on a continuous time linear system, the $(p + 1) \times (q + 1)$ scrolls chaotic attractors can be generated:

$$\begin{aligned} \dot{x} &= y - \sum_{i=1}^q h_i(x) \\ \dot{y} &= -ax + by + a \sum_{i=1}^p h_i(x) \end{aligned} \quad (4)$$

where x and y are two state variables, a and b are system parameters. $h(x)$ is the hysteresis function. $h_i(x)$ is the hysteresis series and i is the number of hysteresis. When $a = 1$, $b = 0.0625$, $p = 2$, $q = 1$, a 3×2 -scroll chaos generated by Equation (4) is as shown in Figure 4.

Sampling the chaotic signal system (Equation (4)) [19,20] in space gives an irregular sampling of the signal in

time. In Figure 4, the systems trajectories around any equilibrium point are evolving clockwise and will be switched by either its upper or lower switching lines. If the trajectory is switched by its lower switching lines, a number 0 can be created, and switched by upper switching lines, a number 1 will be recorded. Therefore, a binary sequence, ψ , based on the recorded numbers both in horizontal and vertical direction is obtained. Either 0 or 1 would be recorded depending on the initial conditions when trajectory landed on the basin of attraction of the corresponding equilibrium point. Statistic tests demonstrate that the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit.

In short, the chaos key is the random number sequence generated by the multi-scroll chaos, which is used to XOR the ECG data. Only the server, not the patient and the hospital, knows the initial condition. While encrypting and decrypting, both the patient and the hospital know the current key. But the one-time-pad is used in the encryption, which means the key (random sequence generated by chaotic generator) is only used once within a short period of time.

3.3. Secure key exchange

If the chaos key is transmitted in unencrypted form, then it can fall under wrong hand and the whole system becomes vulnerable to security threats (e.g., man in the middle attack, spoof attack, etc.). Therefore, secured transmission of the chaos key must be in place. For our implementation of secured key exchange of the chaos key among the patient's mobile phone, the hospital and the chaos key server, we have implemented a variant of Diffie Hellman key exchange mechanism. Figure 5 shows the three step process. The patient first visits the hospital or the health monitoring service provider (ideally during the registration phase, when the monitoring software is installed into the patient's mobile phone) to download the common base g and prime number, P from the hospital server via Near Field Communication (NFC) protocol (<http://www.nfc-forum.org>). For this scenario, the chaos key server is implemented within the hospital. Both g and P common for the mobile phone and the hospital server and they are only updated with patient's visit in the hospital through NFC touch scheme. For our demonstration we have used the NFC kit supplied by Nexpert (<http://www.nexpert.com>) along with NFC enabled mobile phone (Figure 6).

Next, the mobile phone computes A using mobile's secret key a (Equation (5)) and transmits the value over public network to the hospital. The hospital calculates B using hospital's secret key b and transmits B over the Internet.

Later on, both the parties (mobile phone and the hospital server) reaches the same shared key, K , (refer to Equations (8), (7)) since g^{ab} and g^{ba} are equal MOD P . The secret keys are generated by the mobile phone and the hospital at a predefined interval and when it is done only A and B values are communicated over unsecured media. The secret

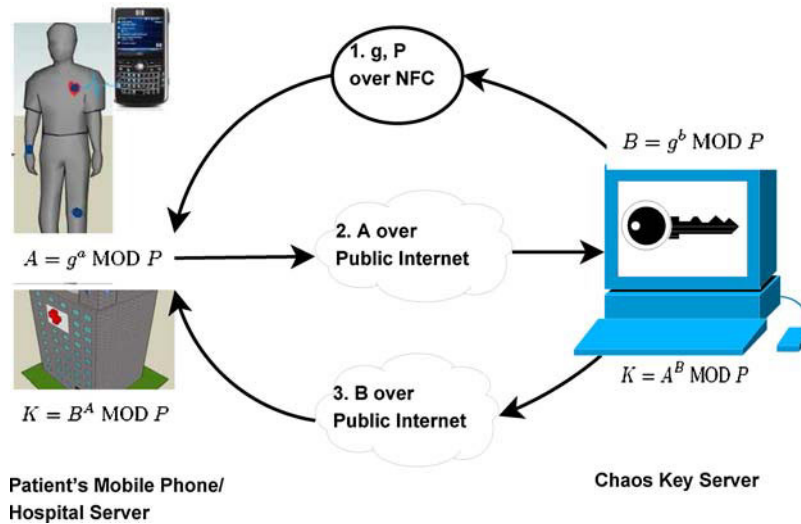


Figure 5. Three step key exchange implementation between the patient's mobile phone and the chaos server.

key a and b are never released over the unsecured media (so as g and P).

The chaos keys are always XORed against the shared secret key K before sending to the mobile phone (from the chaos server). Once the mobile phone receives the chaos key (encrypted), it decrypts the chaos key (encrypted) by XORing the shared secret key K again. *Discussions:* As a chaos random sequence can be very long, one initial condition or seed can generate many cryptographic keys. Therefore, it is feasible to use a chaos cryptographic key only for one session which generates a virtual one-time pad. For more secured key distribution framework that can also comply with HIPAA standard, one can consider our recent hybrid PKI key distribution scheme [21]

$$A = g^a \text{ MOD } P \tag{5}$$

$$B = g^b \text{ MOD } P \tag{6}$$

$$K = A^B \text{ MOD } P \tag{7}$$

$$K = B^A \text{ MOD } P \tag{8}$$

4. EXPERIMENTATION AND RESULTS

Table II shows how we performed XOR operations for encrypting the Chaos Key with a Shared Secret Key (variant of Deffi Hellman) and Original ECG with the Chaos Key. As discussed earlier Chaos Key is encrypted for secured key distribution purpose from the chaos server to the Patient's mobile phone and the hospital server. On the other hand, ECG is encrypted for preserving patient's privacy (while transmitting over the public Internet) by XORing chaos key with the original ECG. An ECG looks like, 0.175, 0.180, 0.165 . . . The Chaos Key server generates a vector of the same length (e.g., 0.719, 0.180, 0.890, . . .), so that ECG can be encrypted with one time padding. Even though both the chaos key and the ECG signal are in three digit precision format of decimal values, for simplifying calculation both the vectors were multiplied by 1000 for converting them into integer values. Once both the Original ECG and Chaos Key are converted into integer values the XOR operation becomes straight forward for them. As an example, 175 (or binary 000010101111) and 719 (binary 001011001111) becomes 608 (binary 001001100000) after XORing. Before, releasing on to the public media (e.g., Internet) this encrypted ECG value is transformed to three digit precision decimal (e.g., 0.608). It should be noted that the left most bit (12th bit) of the binary ECG sample denotes the sign of the ECG (e.g., 1 means negative sample and 0 means positive sample) for our implementation.



Figure 6. NFC communication with NFC enabled mobile phone.

Table II. XORing technique for an example case.

Chaos key	Shared secret key	Encrypted chaos key	Original ECG	Encrypted ECG
0.719	341	0.922	0.175	0.608
0.180	341	0.481	0.180	0.000
0.890	341	0.559	0.165	0.991
⋮	341	⋮	⋮	⋮

Similarly, the chaos key vector is converted to series of integer values before performing XOR with the shared secret key (341 according to the example case in Table II).

4.1. Data collection

Few entries of Normal Sinus Rhythm Database (NSRDB) [22] were used to validate our proposed model of ECG-based person identification. From each entry four randomly selected ECG segments were used for our experimentations. The sampling frequency of the collected ECG signals was 128 Hz. The duration of each of the ECG segments was 5 s (i.e., 5×128 or 640 samples in one ECG segment). The resolution of the ECG was 10 bits. Therefore, each ECG segments looked like a vector with 640 elements and about three digit precision after decimal.

4.2. Simulation of patient mobile

In an ideal case, patient’s ECG will be collected from an ECG acquisition device (such as Alive Heart Monitor [4]) and ECG packets will be directed from the acquisition device towards patient’s mobile phone. However, for our

experimentation, we did not collected ECG signal from a real person. Instead, we stored publicly available ECG packets [22] within the resource folder of our Java 2 Platform Micro Edition (J2ME) program. To simulate the patient’s ECG coming from the acquisition device, these publicly available ECG packets were picket up the J2ME program (i.e., MIDlet) [23]. As seen in Figure 7, the MIDlet (or J2ME program) applies XOR operation between the chaos key and the ECG signal. The mobile phone requests the chaos key from the simulated chaos key server using HTTP query string process (e.g., <http://localhost/chaosserver/cs.asp?phoneID=319000392>). It should be noted that query string process was used for demonstration and simulation purpose only. In real scenario, HTTPS (secured HTTP) or other secured protocols will be utilized for receiving the chaos key from the server.

4.3. Simulation of chaos key server

To simulate the chaos server, we developed an ASP.Net project using Microsoft Visual Studio 2006. The Active Server Pages (ASP) pages were hosted under localhost

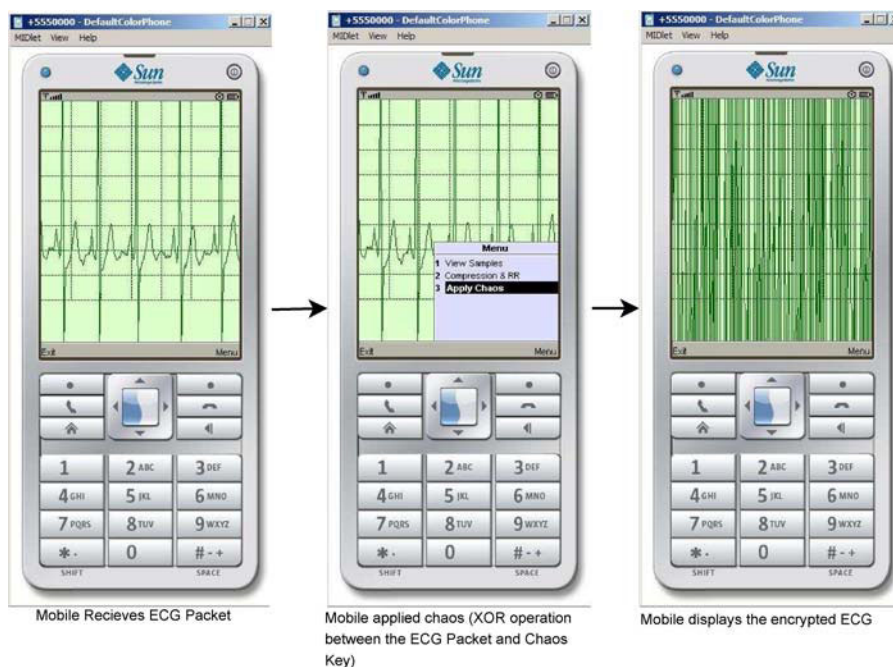


Figure 7. Enrolment and recognition ECG of 16272 and 16273.

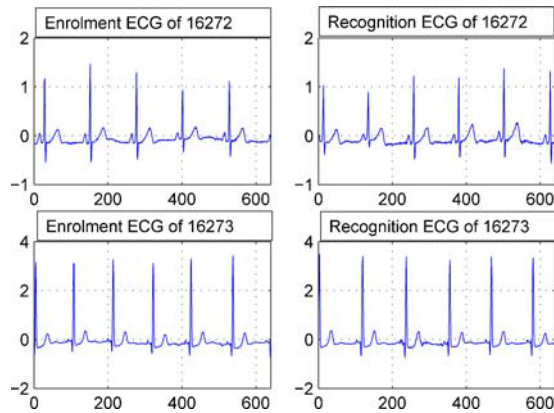


Figure 8. Enrolment and recognition ECG of 16272 and 16273.

maintained by windows Internet Information Server (IIS). The purpose of this simulated chaos key server is simple, supply a chaos key to a valid requester (subscribed patient's mobile phone).

4.4. Simulation of hospital server

The simulated hospital server requests the same chaos key from the chaos server. To obtain the same chaos key, the hospital server has to provide the phoneID of the subscribed patient (e.g., <http://localhost/chaosserver/cs.asp?phoneID=319000392>). This phoneID can be subscription ID as well. This id basically identifies subscribed patient.

After obtaining the chaos key and the encrypted ECG signal, hospital server applies XOR operation to retrieve the original ECG signal.

4.5. Simulation of man in the middle attack

As we already know, using template-matching techniques (e.g., cross correlation (CC), percentage root mean square deviation (PRD), wavelet distance measurement (WDM)), recognition ECG packet can be matched with enrolment ECG packet to confirm that both the ECG packets belongs to the same person. Therefore, if the ECG transmitted in an unsecured manner, then the man in the middle (or intruder) can get hold of the recognition ECG and use that recognition ECG to falsely identify him to gain access to a secured biometric authentication (ECG based) system. Figure 8 shows the enrolment and recognition ECG of two MIT BIH entries (16272, 16273) used with existing biometric system (our previous research in ECG-based biometric [11,13–15]). Using these available ECG biometric techniques, it is confirmed that they belong to the same person. Therefore, if the man in the middle receives the recognition ECG, he will be able to reproduce the same outcome in identifying the person.

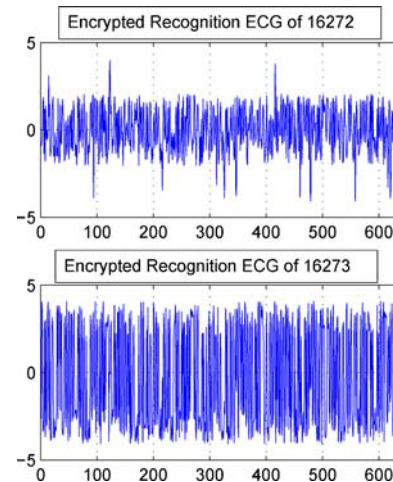


Figure 9. Encrypted recognition ECG segments of entry 16272 and 16273. Identity of the person is concealed and cardiovascular condition is unknown.

Now instead of sending unencrypted ECG packet, if chaos-based encryption is used on the recognition ECG packets of Figure 8, then it would appear as Figure 9. Applying all the existing ECG-based biometric techniques ([7,8,11–15,24–27]), identity of the person could not be revealed (unsuccessful match).

As an example, with our implementation of existing biometric (PRD and WDM [24]) on both enrolment and recognition ECG of 16273 (Figure 8), we observe the following values:

$$\begin{aligned} \text{PRD} &= 14.0793 \\ \text{WDM} &= 46.9056 \end{aligned}$$

After we apply chaos on the recognition ECG, the PRD and WDM (distances [24]) becomes substantially higher.

$$\begin{aligned} \text{PRD} &= 61.769 \\ \text{WDM} &= 1869.0935 \end{aligned}$$

Higher distance between the enrolment ECG and chaos-based obfuscated recognition ECG clearly shows that person cannot be identified using some of the existing ECG-based biometric techniques (such as PRD and WDM [24]).

PRD provides a measurement of dissimilarity between two signals $e(i)$ and $r(i)$ (as shown in Equation (9) [11,24]).

$$\text{PRD} = \sqrt{\frac{\sum_{i=1}^N [e(i) - r(i)]^2}{\sum_{i=1}^N [e(i)]^2}} \times 100 \quad (9)$$

Similarly, WDM also provides an efficient measurement of distance between two signals, established with normalized difference between wavelet coefficients of the two signals. With $\lambda^{q,v}$ being the detail coefficient v from the q th level of decomposition, WDM can be represented by Equation (10) [11,24]. ξ is used to overcome overemphasis

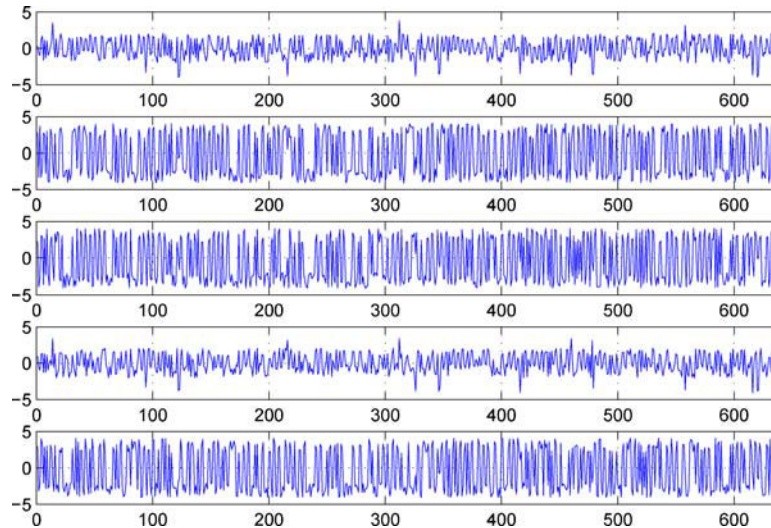


Figure 10. Chaos-based encrypted ECG segments of some other ECG segments, collected from entry 16272, 16273, 16420, 16265, 17453 ([22]).

generated by differences in relatively small wavelet coefficients.

$$\text{WDM} = \sum_{q=1}^Q \sum_{v=1}^V \frac{|\lambda_0^{q,v} - \lambda_z^{q,v}|}{\max(|\lambda_0^{q,v}|, \xi)} \quad (10)$$

Similarly, Figure 10 shows some other encrypted ECG packets, from which the biometric matching remained unsuccessful. These experimentations uphold high level of security that can be achieved harnessing the power of true random numbers generated by chaos.

5. DISCUSSION

As mentioned in Section 2 of this paper, our previous method depicted in Reference [4] raises the security strength of three layer ECG encryption several times higher than conventional encryption mechanisms like AES or DES. This enormously higher security strength was originated essentially from three layer permutation cipher structure (i.e., $4 \times 256! \times 256!$, refer to Reference [4] for detail calculations). For estimating the security strength of this multi scroll chaos based encryption algorithm, we have to take into account the possibilities of values (i.e., the chaos key sample values) that may occur in for a particular sample point. An ECG sample with 10 bit resolution (three digit precision after zero) and 500Hz sampling frequency, can have 10 000 different values (if the value ranges between +ve 5 mV and -ve 5 mV) and chaos value can be a random number within this range. Since there are 500 sample in a second, the search space of finding a correct 1 s ECG segment would be $10\,000^{500} = 10^{2000}$. To obtain the number of years required for a complete exhaustive search for a computer that can check a billion billion (10^{18}) combination

per second would be $\frac{10^{2000}}{3600 \times 24 \times 365 \times 10^{18}}$ years. The possibility of finding the correct combinations would be half of that time. Therefore, the security strength provided the multi scroll chaos is substantially higher (AES requires about only 3×10^{51} years to exhaust a search space of 256 bit key, utilizing the same computational expense). Therefore, while achieving faster computation on mobile platform, the proposed chaos-based ECG encryption does not compromise the security strength.

Existing algorithms like AES or DES indulge computational burden on regular mobile platform [28]. Even though the high end state-of-the-art mobile platform runs on faster processor, if we are to adopt AES or DES, then all the CVD patients require to switch to high end mobile devices, surrendering their existing mobile phone (which may run on J2ME CLDC 1.1 with limited computational resources [29]). This would be feasible, only if the presented algorithm is beaten on security strength. However, the chaos-based truly random key provides substantially higher security strength while running at least 22 times faster than existing algorithms [28].

6. CONCLUSION

This paper proposes the innovative idea of harnessing the power of multi-scroll chaos to encrypt ECG packets on the fly. Since, the mobile device only needs to perform a single operation (XOR) to encrypt an ECG packet, the proposed ECG encryption method is deemed to be the fastest according to the literature (reported) and to the best of our knowledge. While running it on HP 912 Smartphone (.Net Platform) and Nokia N95 (J2ME Platform) the proposed encryption was found to be 18 times faster than [3,4], 25 times faster than [6,9], and 31 times faster than [5,10].

Our experimentation reveals that the encrypted ECG packets generated by the proposed system, does not reveal the identity of a person, as well as cardiovascular details, since random noise is XORed with the original ECG packet. In Reference [18], the author concluded that more complex attractors such as n -scrolls attractors may further improve unpredictability and the based on our previous research in References [19,20], we have implemented multi scroll chaos. Therefore, the noises generated by the proposed implementation harnesses certain degree of unpredictability.

Due to the fast nature of encryption/decryption process, the proposed chaos-based encryption technique can be highly suitable for wireless telecardiology application, where every second counts towards saving life [30].

ACKNOWLEDGEMENTS

This research was partially supported by ARC discovery grant DP0985838.

REFERENCES

1. Health insurance portability accountability act of 1996 (hipaa), centers for medicare and medicaid services, 1996. Available online at: <http://www.cms.hhs.gov/hipaageninfo>, [Accessed in 2008].
2. Hu J, Han F. A pixel-based scrambling scheme for digital medical images protection, *Journal of Network and Computer Applications*. 2009; **32**: 788–794.
3. Sufi F, Fang Q, Khalil I, Mahmoud SS. Novel methods of faster cardiovascular diagnosis in wireless telecardiology. *IEEE Journal on Selected Areas in Communications* 2009; **27**(4): 537–552.
4. Sufi F, Khalil I. Enforcing secured ecg transmission for realtime telemonitoring: a joint encoding, compression, encryption mechanism. security and communication networks. *Security and Communication Networks* 2008; **1**(5): 389–405.
5. Sufi F, Khalil I. A new feature detection mechanism and its application in secured ecg transmission with noise masking. *Journal of Medical Systems* 2009; **33**(3): 121–132.
6. Sufi F, Mahmoud S, Khalil I. A novel wavelet packet based anti spoofing technique to secure ECG data. *International Journal of Biometrics* 2008; **1**(2): 191–208.
7. Biel L, Petersson O, Philipson L, Wide P. Ecg analysis: a new approach in human identification. *IEEE Transaction on Instrumentation and Measurement* 2001; **50**(3): 808–812.
8. Israel SA, Irvine JA, Cheng A, Wiederhold BK. Ecg to identify individuals. *Pattern Recognition* 2005; **38**(1): 133–142.
9. Sufi F, Mahmoud S, Khalil I. A wavelet based secured ecg distribution technique for patient centric approach. *5th International Workshop on Wearable and Implantable Body Sensor Networks*, Hong Kong, China, 2008.
10. Sufi F, Mahmoud S, Khalil I. A new obfuscation method: a joint feature extraction & corruption approach. *5th International Conference on Information Technology and Application in Biomedicine*, Shenzhen, China, 2008.
11. Sufi F, Khalil I, Hu J. Chapter 17: ECG-Based Authentication, Handbook of Information and Communication Security, Stavroulakis P, Stamp M (Eds.), Springer 2010, ISBN978-3-642-04116-7 (Print) 978-3-642-04117-4 (Online) DOI10.1007/978-3-642-04117-4; 309–331
12. Wubbeler G, Stavridis M, Kreiseler D, Boussejot RD, Elster C. Verification of humans using the electrocardiogram. *Pattern Recognition Letters* 2007; **28**: 1172–1175.
13. Sufi F, Khalil I, Habib I. Polynomial distance measurement for ECG based biometric authentication. *Security and Communication Networks*, 2009 (in press). DOI: 10.1002/sec.76
14. Khalil I, Sufi F. Legendre polynomials based biometric authentication using qrs complex of ECG. *International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008 (ISSNIP 2008)*, December 2008; 297–302.
15. Sufi F, Khalil I. An automated patient authentication system for remote telecardiology. *International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008 (ISSNIP 2008)*, December 2008; 279–284.
16. Clifford GD, Azuaje F, McSharry PE. *Advanced Methods and Tools for ECG Data Analysis*. Artech House Inc: Norwood, MA, USA, 2006.
17. Dachsel F, Schwarz W. Chaos and cryptography. *IEEE Transactions on Circuits and Systems-I* 2001; **48**(12): 1498–1509.
18. Yalçın ME, Suykens JAK, Vandewalle J. True random bit generation from a double-scroll attractor. *IEEE Transactions on Circuits and Systems-I* 2004; **51**(7): 1395–1404.
19. Han F, Yu X, Feng Y, Hu J. On multi-scroll chaotic attractors in hysteresis-based piecewise linear systems. *IEEE Transactions on Circuits and Systems-II* 2007; **54**(11): 1004–1008.
20. Han F, Yu X, Wang Y, Feng Y, Chen G. N-scroll chaotic oscillators by second-order systems and double-hysteresis blocks. *IEE Electronics Letters* 2003; **39**: 1636–1637.

21. Hu J, Chen H, Hou T. A hybrid public key infrastructure solution (hpki) for hipaa privacy/security regulations. *Special Issue on Information and Communications Security, Privacy and Trust: Standards and Regulations*. Computer Standards & Interfaces, Elsevier, 2010; **32**(9): 274–280.
22. Physiobank: Physiologic signal archives for biomedical research. Available online at: <http://www.physionet.org/physiobank/> [Accessed in 2009].
23. Sufi F. Mobile phone programming java 2 micro edition. *Proceedings of the 2007 International Workshop on Mobile Computing Technologies for Pervasive Healthcare*, Philip Island, Melbourne, December 2007; 64–80.
24. Chan ADC, Hamdy MM, Badre A, Badee V. Wavelet distance measure for person identification using electrocardiograms. *IEEE Transaction on Instrumentation and Measurement* 2008; **57**(2): 248–253.
25. Poon CCY, Zhang YT, Bao SD. A novel biometric method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communication Magazine* 2006; **44**(4): 73–81.
26. Bui FM, Hatzinakos D. Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling. *EURASIP Journal on Advances in Signal Processing* 2008; **2008**: Article ID 529879.
27. Irvine JM, Wiederhold BK, Gavshon LW, *et al.* Heart rate variability: a new biometric for human identification. *International Conference on Artificial Intelligence*, Las Vegas, Nevada, 2001; 1106–1111.
28. Filho B, Viana W, Andrade R, Monteiro A. Pearl: a performance evaluator of cryptographic algorithms for mobile devices. *MATA 2004, LNCS 3284*, 2004; 275–284.
29. Yuan MJ. *Enterprise j2me: Developing Mobile java*. Prentice Hall PTR: Upper Saddle River, NJ, c2004.
30. Luca GD, Suryapranata H, Ottervanger JP, Antman EM. Time delay to treatment and mortality in primary angioplasty for acute myocardial infarction: every minute of delay counts. *Circulation* 2004; **109**: 1223–1225.