Pseudo Random Data Stream Generation for Data/Images Protection in Ubiquitous Computing Environment

Fengling Han[1], Yong Feng[2], Naif Saeed Alzahrani[1], Kai Xi[1] and Jiankun Hu[3]

[1]School of Computer Science & IT
Royal Melbourne Institute of Technology
Melbourne, VIC 3001, Australia
{fengling, Kai@cs.rmit.edu.au}

[2]Department of Electrical Engineering
Harbin Institute of Technology
Harbin, 150001, China
{yfeng@hit.edu.cn}

[3]School of Engineering and Information Technology, UNSW@ADFA
Canberra, ACT 2600, Australia
{J.Hu@adfa.edu.au}

***Abstract*— A data stream generated from hysteresis-based multi-scroll chaos is proposed in this paper. The mathematical model of the multi-scroll chaotic attractor is a continuous-time linear third-order system with a feedback of hysteresis-series. The pseudo random data stream is generated from the state values of the third-order systems at the instance of hysteresis switching. Thanks to the complicated dynamical behavior of the multi-scroll chaotic attractor, the resulted data stream demonstrates highly unpredictability which is ideal for security use. Due to the simplicity of system model, the data stream can be generated in resource limited environment, such as mobile computing environment and wireless sensors. The data stream generation has been implemented in mobile phones with J2ME. It has the potential to be used as one time pad key in protecting information in ubiquitous computing environment. The resulting cipher can achieve high security strength with low cost.**

Keywords-chaos; mobile; security; ubiquitous computing

I. INTRODUCTION

Mobile devices possess the capability of being always on and always connected whether the person is in a fixed location or on travel [1, 2]. Mobile commerce (m-commerce) is known as mobile electronic commerce or wireless electronic commerce which is defined as the conduct of business transactions over the Internet-enabled wireless devices [1]. M-commerce has the capability of accessing information ubiquitously at anytime and anywhere while maintains the lowest cost because the service is based on mobile devices and wireless communication infrastructure. The potential prospect applications of m-commerce are in healthcare [2-5], finance [6-8] and government service [9, 10] domains.

Mobile devices are replacing desk personal computer for ubiquitous and pervasive applications address the convenience. The portability of mobile devices making them attractive but also increases the risk of being lost or stolen which may expose data to opponents. In addition, majority of the m-commerce is delivered via public network which is considered as convenient, cost-effective, but insecure. The security of data/information storage and transmission has become more concerned not only by government and law enforcement but also by researchers and industries.

Mobile healthcare (m-healthcare) or ubiquitous healthcare (u-healthcare) typically refers to portable devices with the capability to create, store, retrieve, and transmit data in real time between end users for the purpose of improving patient safety and quality of care [3]. Providing convenient health facilities at a low cost has always been rather challenging for healthcare communities. Along this line, mobile ubiquitous monitoring (MUM) is a trend of healthcare in which information is delivered by communication infrastructures among end users via public network. On the other hand, medical applications often deal with patients′ personal data/information that are confidential and require protection against unauthorized access [3, 4]. However, the existing ubiquitous healthcare monitoring systems either implement a monitoring function without security consideration due to constraint of size, cost and processing ability of wireless sensors [11-14], or employ expensive security procedures theoretically for privacy protection [16-18]. MUM schemes are convenient. However, the computational power of mobile devices is significantly less than their desktop counterpart. The success of MUM depends heavily on the security of the underlying mobile technologies, and certain risks are involved with mobile communications because network carriers do not provide a consistent level of encryption that meets security requirements [18]. The wide deployment of MUM will be brought into practice only if the potential customers trust the service, mainly the security of the service.

This paper proposes a pseudo random data stream generation scheme which could be used in data/images protection in ubiquitous monitoring applications. The data stream is generated from a multi-scroll chaotic attractor which is composed of a continuous linear third-order system and a hysteresis-series. Due to the complex dynamic behavior of chaotic systems and the simple model of the multi-scroll chaotic attractor, the produced data stream is pseudo random and can be implemented easily in resource constrained environment, such as mobile devices and wireless sensors. This

This work is partially supported by ARC Discovery Grant Australia (DP0985838), and the National Natural Science Foundation of China (61074015).

is desired to be used as cryptography key in ubiquitous monitoring applications.

This paper is organized as follow: section II introduces the multi-scroll chaotic attractors generated from a third-order linear system with feedback of hysteresis-series. Method for pseudo random data stream generation is proposed in section III. Application of the data stream in mobile ubiquitous monitoring application for key generation is demonstrated in section IV. Finally, conclusions are drawn in section V.

II. MULTI-SCROLL CHAOS FROM LINEAR THIRD-ORDER SYSTEMS WITH FEEDBACK OF HYSTERESIS-SERIES

Chaotic dynamics can produce unpredictable behavior with deterministic equations. Chaos-based cryptography has been studied widely [19-22]. In this section, the hysteresis-based chaotic attractor from autonomous continuous-time linear third-order system with hysteresis control is introduced [21]. This system will be further used to generate pseudo random data stream in this research.

A. Hysteresis-Based Multi-Scroll Chaotic Attractors

A basic hysteresis unit, $h(x)$, is described as:

$$h(x)=\begin{cases}1 & x>0 \quad \dot{x}<0\\ 0 & x<1 \quad \dot{x}>0\end{cases}. \tag{1}$$

A hysteresis-series is shown in Fig.1 and is described as:

$$h(x,p)=\sum_{i=1}^{p}h_i(x). \tag{2}$$

where x is the input, and p is the number of hysteresis.

A multi-scroll chaotic attractor can be generated from autonomous continuous-time linear third-order systems with feedbacks control of hysteresis-series [21]:

$$\begin{cases}\dot{x}=y-v\\ \dot{y}=z\\ \dot{z}=-ax-by-cz+au+bv\\ u=h(x,p)\\ v=h(y,q)\end{cases}. \tag{3}$$

where x, y, z are state variables; a, b, c are constants, p, q are the number of hysteresis-series feedback in the direction of x and y, respectively. The system (3) has $(p+1)\times(q+1)$ equilibrium points located in $(p+1)\times(q+1)$ subspaces which are given by:

$$O_{xyz}=[(i,j,0)|\ 0\le i\le p,\ 0\le j\le q]. \tag{4}$$

The characteristic equation of system (3) is:

$$\lambda^3-c\lambda^2-b\lambda+a=0. \tag{5}$$

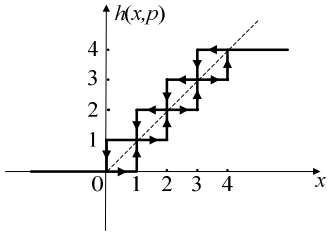


Figure 1. A hysteresis-series has four hysteresis.

Let $\lambda=\Lambda-c/3$. Substituting it into Eq. (5), then

$$\Lambda^3+(b-\frac{1}{3}c^2)\Lambda+\frac{2}{27}c^3-\frac{1}{3}bc+a=0. \tag{6}$$

Denoting

$$r=b-\frac{1}{3}c^2,$$

$$s=\frac{2}{27}c^3-\frac{1}{3}bc+a,$$

$$\Delta=\frac{1}{27}ac^3-\frac{1}{108}b^2c^2-\frac{1}{6}abc+\frac{1}{27}b^3+\frac{1}{4}a^2.$$

and solving (6) yields:

$$\begin{cases}\lambda_1=\Lambda_1-\frac{1}{3}c=-\frac{1}{3}c+\sqrt[3]{-\frac{s}{2}+\sqrt{\Delta}}+\sqrt[3]{-\frac{s}{2}-\sqrt{\Delta}}\\ \lambda_{2,3}=\Lambda_{2,3}-\frac{1}{3}c\\ \quad=-\frac{1}{3}c-\frac{1}{2}(\sqrt[3]{-\frac{s}{2}+\sqrt{\Delta}}+\sqrt[3]{-\frac{s}{2}-\sqrt{\Delta}})+j\frac{\sqrt{3}}{2}(\sqrt[3]{-\frac{s}{2}+\sqrt{\Delta}}-\sqrt[3]{-\frac{s}{2}-\sqrt{\Delta}})\\ \quad\equiv\alpha+j\beta\end{cases} \tag{7}$$

Under the conditions $\lambda_1<0$, $\alpha>0$ and $\beta\neq 0$, system (3) will appear chaotic behavior. Or in other words, if (5) has a negative eigenvalue and a pair of conjugate complex eigenvalues with positive real parts, with initial conditions, the multi-scroll chaotic attractors can be generated.

On each subspace $\boldsymbol{W}_i$ $(1\le i\le(p+1)\times(q+1))$, the solutions of system (3) can be obtained as follows:

$$\begin{cases}\mathbf{X}(t)=A_1e^{\lambda t}+e^{\alpha t}(A_2\cos(\beta t)+A_3\sin(\beta t))]\\ \mathbf{Y}(t)=A_1\lambda e^{\lambda t}+e^{\alpha t}[(A_2\alpha+A_3\beta)\cos(\beta t)+(A_3\alpha-A_2\beta)\sin(\beta t)]\\ \mathbf{Z}(t)=A_1\lambda^2e^{\lambda t}+e^{\alpha t}[(A_2\alpha^2+2A_3\alpha\beta-A_2\beta^2)\cos(\beta t)+\\ \qquad(A_3\alpha^2-2A_2\alpha\beta-A_3\beta^2)\sin(\beta t)]\end{cases}. \tag{8}$$

where $X(0)$, $Y(0)$ and $Z(0)$ are the initial conditions, and

$$\begin{cases} A_1 = \dfrac{(\alpha^2+\beta^2)X(0) - 2\alpha Y(0) + Z(0)}{(\lambda-\alpha)^2+\beta^2} \\ A_2 = \dfrac{(\lambda^2 - 2\alpha\lambda)X(0) + 2\alpha Y(0) - Z(0)}{(\lambda-\alpha)^2+\beta^2} \\ A_3 = \dfrac{(\lambda\alpha^2 - \lambda\beta^2 - \lambda^2\alpha)X(0) - (\beta^2 - \alpha^2 + \lambda^2)Y(0) + (\alpha-\lambda)Z(0)}{\beta[(\lambda-\alpha)^2+\beta^2]} \end{cases}.$$

The exact solution of system (3) can be obtained:

$$(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})^T = (x\text{-}i,\ y\text{-}j,\ z)^T \text{ for } \overline{\boldsymbol{X}} \in \boldsymbol{W}_{(i,j)},\ 0 \le i \le p,\ 0 \le j \le q. \quad (9)$$

If p=q=2, and a=1.0, b=0.7, c=0.8, then system (3) has a 3×3-scroll chaotic attractor located on nine subspaces. This *x*-*y*-*u* project is as shown in Fig.2(a). The nine equilibrium points of system (3) are shown in Fig.2(b):

$$E_1(0, 0, 0),\ E_2(1, 0, 0),\ E_3(2, 0, 0);$$

$$E_4(0, 1, 0),\ E_5(1, 1, 0),\ E_6(2, 1, 0);$$

$$E_7(0, 2, 0),\ E_8(1, 2, 0),\ E_9(2, 2, 0).$$

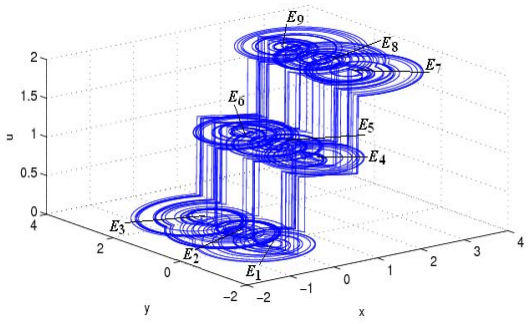
B. Dynamics of the Multi-Scroll Chaotic Attractors

For a given initial values, the trajectory of system (3) diverges spirally (stretching) around its equilibrium point in each subspace until it reaches the boundary of this subspace, then being switched (folded) by hysteresis-series and jumps to one of its neighboring subspace. The linear part of system (3) is unstable. With the switching of hysteresis-series, the system trajectory will be wandering through all the subspaces alternately and repeatedly, after a long enough time, very complex dynamics will be resulted.

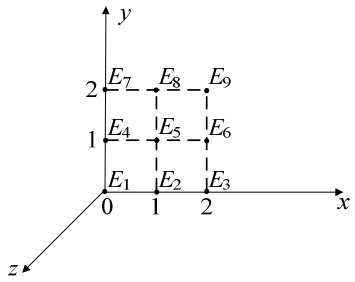
As shown in Fig.1, the hysteresis switching has a rising edge and a falling edge. For a specific input, there are two possible outputs. Roughly speaking, the output of hysteresis depends on both the current state and the history of input. In systems with hysteresis, there is no way to predict the output without knowing the system's current state, and there is no way to know the system's state without looking at the history of the input [24]. This excellent feature is used in creating both chaos and the pseudo random data stream in this research.

In Fig.2(a), the trajectory starts from any initial values within the basin of chaotic attraction, it evolves around one equilibrium point E_i (i =1, …, 9), and will be switched by either an upper switching line SL_U or a lower switching line SL_L then evolves around its neighboring equilibrium point. The location of equilibrium point can be classified as i) corner (E_1, E_3, E_7 and E_9); branch (E_2, E_4, E_6 and E_8); and centre (E_5). The possibility of being switched is different among the nine equilibrium points depending on the location of equilibrium point. The similar evolvement will be repeated again and again. In order to demonstrate the dynamic behavior, the first groups of switching when trajectory starts with an initial condition in Fig.2(a) is illustrated in Table I.

As shown in Table I, there are two possible switching corresponding to two neighboring equilibrium points when trajectory evolves around corner equilibrium points; there are three possible switching around branch equilibrium points; and there are four possible switching around centre equilibrium points.



(a)



(b)

Figure 2. (a) The *x*-*y*-*u* project of a 3×3-scroll attractor. a=1.0, b=0.7, c=0.8, p=2, q=2. (b) Equilibrium points of the attractor.

Remark:

- The three dimensional diagram is only used to help to understand the dynamic process of Eq.(3). In Fig.2 (a), the control signals, u, is the output of hysteresis-series, but not state variable.

TABLE I.
SWITCHING OF TRAJECTORY EVOLVES AROUND EQUILIBRIUM POINTS.

Equilibrium point	Top level subspace	Middle level subspace	Ground level subspace	LOCATION
$E_1(0, 0, 0)$	$u(x)$=1 E_4	$v(y)$=1 E_2		corner
$E_2(1, 0, 0)$	$u(x)$=2 E_7	$u(x)$=1 E_5	$u(x)$=0 E_1	branch
$E_3(2, 0, 0)$		$v(y)$=1 E_8	$u(x)$=1 E_4	corner
$E_4(0, 1, 0)$	$u(x)$=1 E_5	$v(y)$=2 E_3	$v(y)$=0 E_1	branch
$E_5(1, 1, 0)$	$u(x)$=2 E_8	$v(y)$=0 E_4 $v(y)$=2 E_6	$u(x)$=0 E_2	centre
$E_6(2, 1, 0)$	$u(y)$=2 E_9	$v(y)$=0 E_7	$u(x)$=1 E_5	branch
$E_7(0, 2, 0)$	$u(x)$=1 E_6	$v(y)$=1 E_2		corner
$E_8(1, 2, 0)$	$u(x)$=2 E_9	$v(y)$=1 E_5	$u(x)$=0 E_3	branch
$E_9(2, 2, 0)$		$v(y)$=1 E_8	$u(x)$=1 E_6	corner

- The definition of corner, branch and centre equilibrium points can be expanded to any dimension of multi-scroll attractors described by (3). For an $m\times n$ multi-scroll attractor, the number of corner equilibria is 4, the number of branch is $2\times(m+n-4)$, and the number of centre is $m\times n+4-2\times(m+n)$.

III. Pseudo Random Data Stream Generation

Inspired by the work in [20] which creates true random data from double-scroll chaotic attractor, a binary bit has been produced from the multi-scroll chaotic attractor by sampling the output of hysteresis switching in a hysteresis-based continuous-time linear second-order systems [23]. More scrolls would produce higher complex dynamic behaviors which can further improve unpredictability [20]. In this paper, the data stream is collected by sampling the state values corresponds to the hysteresis switching, rather than the one bit hysteresis switching value. And the systems model is based on a third-order system rather than the second-order system with feedback of hysteresis. In this way, a bulk size of data could be produced in a short period of time.

As demonstrated in the previous section, with the evolvement of the system trajectory around each equilibrium point, it will be switched by either an upper switching line corresponding to the rising edge of hysteresis or a lower switching line corresponding to the falling edge of hysteresis. A trajectory starts from P_1(1.2, 1.36) (in the middle of the ground level) runs outgoing exponentially in the direction of counter clockwise, then being switched by u=2 at point 2. After that, the exponential outgoing of trajectory will be switched by v=1 at point 3. The similar motion repeats until the trajectory evolving to point 15. The characteristics of switching points are summarized in Table II. The coordinates of switching points P_i (i =1, …, 15) include one hysteresis switching value and one corresponding state value. The hysteresis switching can be obtained from $u_1(x)$, $u_2(x)$, $v_1(y)$ or $v_2(y)$. That is:

TABLE II.
STATE VALUES OF THE SWITCHING POINTS.

Switching point	Switched value	Coordinate (x_i, y_i)	Corresponding State value
1		P_1 (1.2, 1.36)	
2	$v_2(y)$=2	P_2 (–0.3776, 2)	x_2 = –0.3776
3	$u_1(x)$=1	P_3 (1, 3.1581)	y_3 = 3.1581
4	$v_2(y)$=1	P_4 (1.1499, 1)	x_4 = 1.1499
5	$u_1(x)$=0	P_5 (0, 0.6983)	y_5 = 0.6983
6	$v_2(y)$=2	P_6 (–0.3291, 2)	x_6 = –0.3291
7	$u_1(x)$=1	P_7 (1, 2.9873)	y_7 = 2.9873
8	$u_1(x)$=0	P_8 (0, 1.5320)	y_8 = 1.5320
9	$u_1(x)$=1	P_9 (1, 2.8252)	y_9 = 2.8252
10	$u_2(x)$=2	P_{10} (2, 2.7957)	y_{10} = 2.7957
11	$v_2(y)$=1	P_{11} (2.8456, 1)	x_{11} = 2.8456
12	$v_1(y)$=0	P_{12} (2.2223, 0)	x_{12} = 2.2223
13	$u_1(x)$=1	P_{13} (1, –0.7354)	y_{13} = –0.7354
14	$u_1(x)$=0	P_{14} (0, –0.5656)	y_{14} = –0.5656
15	$v_1(y)$=1	P_{15} (–0.3417, 1)	x_{15} = –0.3417

1) with feedback of state variable x

- either "0" or "1" from the first hysteresis unit $u_1(x)$;
- either "1" or "2" from the second hysteresis unit $u_2(x)$.

2) with feedback of state variable y

- either "0" or "1" from the first hysteresis unit $v_1(y)$;
- either "1" or "2" from the second hysteresis unit $v_2(y)$

The corresponding state values of first eight switching are rounded to fourth digit and recorded as: x_2 = –0.3776, y_3 = 3.1581, x_4 = 1.1499, y_5 = 0.6983 and x_6 = –0.3291, y_7 = 2.9873, y_8 = 1.5320 and y_9 = 2.8252. The state values correspond to the hysteresis switching can be recoded and encoded. The data collection of the state values is performed as follows:

- Recording y when points switched by $u_1(x)$= 0, 1 and $u_2(x)$=1 or 2 (points 3, 5, 7, 8, 9, 10, 13, 14).
- Recording x when points switched by $v_1(y)$= 0, 1 and $v_2(y)$=1 or 2 (points 2, 4, 6, 11, 12, 15).

Looking back to Table II, the state values recorded with the first four hysteresis switching are x_2, y_3, x_4, y_5. With the evolvement of trajectory, it will be switched by v=2, u=1, u=0, u=1 and u=2 consecutively at points 6, 7, 8, 9 and 10. Then the recorded value followed are x_6, y_7, y_8, y_9, y_{10}. During the first fourteen switching, there are six values of x and eight values of y being recorded. Note that the sequence of recorded values of state is random. Furthermore, on what type of switch (hysteresis-series u or v, value 0, 1 or 2) and what value will be recorded (x or y) after being switched by point 15 is unpredictable. This will greatly increase the entropy of the recorded data.

The values of element k_i can be solved by Eq.(3) with the following conditions:

$x = x \mid y$=0, corresponds to points 12;
$x = x \mid y$=1, corresponds to points 4, 11 and 15;
$x = x \mid y$=2, corresponds to points 2 and 6;
$y = y \mid x$=0, corresponds to point 5, 8 and 14;
$y = y \mid x$=1, corresponds to point 3, 7, 9 and 13;
$y = y \mid x$=2, corresponds to points 10.

Remark:

- If a random bit sequence is collected using the method proposed in [23], a 14-bit stream {11001101 100001} is recorded with the 14 switchings. It will take a long time to collect a long enough data stream which is not ideal for real-time application.
- With the proposed random data stream generation scheme in this sub-section, a 14×19-bit data stream is generated as $\{ k_i \} = \{x_2, y_3, x_4, y_5, x_6, y_7, y_8, y_9, x_{10}, x_{11}, y_{12}, y_{13}, x_{14}, x_{15}\}$ = {–0.3776, 3.1581, 1.1499, 0.6983, –0.3291, 2.9873, 1.5320, 2.8252, 2.7957, 2.8456, 2.2223, –0.7354, –0.5656, –0.3417} which contains much more information.

Compared with the 14-bit stream generated in [23], the proposed data stream generation in this research is sampling the state values of the systems rather than the switching value

of hysteresis-series which is more efficient. In addition, the linear part of the hysteresis-based system for data stream generation is third-order systems while a linear second-order system is employ in [23]. On the whole, both the system model and the resulted data stream are more complex than our previous work.

IV. TEST AND APPLICATION

Information security has become more and more important in the modern society. Hence, there must be a mechanism to guarantee that the data/information sampled in ubiquitous monitoring environment are secure and can only be accessed by people who have the authority. In this section, the security of the data stream generation is valued; then the potential application of this data stream in ubiquitous monitoring is illustrated.

A. Distribution of the Pseudo Random Data Stream

The data stream is collected from the state values at the instance of hysteresis switching with the evolvement of system trajectory. The output of hysteresis-series u and v are among "0", "1" or "2" which is determined by the equilibrium points on both horizontal and vertical directions. The distribution of hysteresis switching with long enough time simulation is performed. Two groups of data with around 2,500 and 5,000 times of switching are compared as follows:

- The ratio of trajectory being switched by $u_1(x)$ and $u_2(x)$ are 30% each, and being switched by $v_1(y)$ and $v_2(y)$ are 20% each.
- There is one difference between the number of rising edge and falling edge sometimes. But in the long run, the distribution of "1" and "0" is half each because there is one rising edge and one falling edge in a hysteresis unit if long enough data is sampled.

The evenly distribution of "1" and "0" demonstrates a good statistical characterize. We can conclude that the data stream generation proposed in this section has the following features:

- The collected data stream is pseudo random, it is complex and unpredictable which is guaranteed by the feature of chaos.
- The chaotic trajectory covers almost all the state space. The state values being sampled have a large space and can be any point inside the chaotic basin of attraction.
- Even if the state values are know to the opponent, it is impossible to link the state values to corresponding equilibrium points or the system parameters.

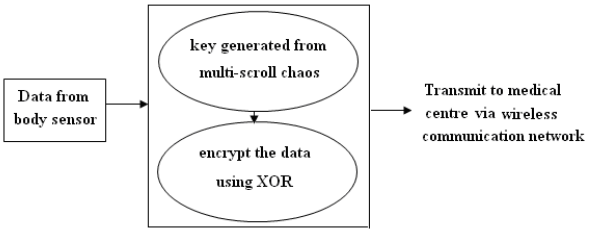


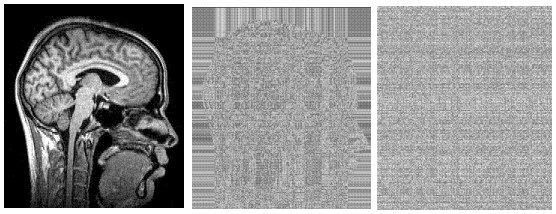
Figure 3. Mobile gateway of ubiquitous monitoring.

B. Protection of Data in Ubiquitous Monitoring Application

Resources in mobile devices are constrained. However, ubiquitous monitoring usually produces huge data from the monitoring sensors. The sampled data is usually encrypted then sent to server where having strong computational resource to analyses the data [25]. The mobile gateway of ubiquitous monitoring from, such as, ECG sensor, blood pressure, environment temperature and humidity, water level, etc. is shown in Fig.3. Inside the mobile gateway, the cryptographic key is extracted from the data stream generated in previous section. This key is used to encrypt the data collected from the site sensor with simple XOR operation. Then the encrypted data is sent to centre server via wireless communication network for further processing.

A digital medical image protection with key generated from the state values at the instance of hysteresis switching from the multi-scroll chaotic attractors are demonstrated in Fig.4. The image in Fig.4(a) is converted into its corresponding binary image. Three rows are chosen as seed row (SR) and three columns as seed column (SC). The selection of the SR and SC is based on the key which is extracted data stream proposed in this paper. The XOR operation is applied on each row of the binary image using SR except the SRs; and the XOR operation also applied on each column of the image using SC except the SCs. This is the one round encryption. After one round XOR operation, the scrambled image is as shown in Fig.4(b) in which a pattern exists.

The pattern could disappear if the image scramble process is repeated for more rounds. In each round, different three rows and three columns are selected as SR and SC which is derived from the pseudo random data stream proposed in section III. After five rounds XOR operation, the encrypted image is as shown in Fig.4(c) which is fully scrambled. In the procedure of data scrambled, there is no information lost because the mechanism is XOR operation.



(a) (b) (c)

Figure 4. Digital medical image encryption with the key derived from data stream in section III. (a) Original DMI; (b) Encrypted image with one round XOR; (c) Encrypted image with 5 rounds XOR.

To decrypt the image in Fig.4(c), it is necessary to know the encryption key. However, it is very difficult to compute the key based on chaos theory if one does not have all the detail information: i) exact parameters of the linear part; ii) the structure and parameters of the hysteresis-series; iii) initial conditions of the trajectory; and iv) how the data stream is sampled; and v) how the sampled values are encoded. The receiver will be able to decrypt the image only if they know all the details of the key used for XOR operation as well as the round of operation.

The data stream generation and the XOR operation have been implemented in mobile phone with J2ME. And Java is used for the purpose of image demonstration.

The advantage of employing mobiles in the proposed algorithm is the ease of exchanging data within a hospital environment and the fact that they can be transported easily to different locations wirelessly without the need of using larger devices. Moreover, a mobile device requires less power than computers. And the most important issue is that this encryption is lose-less which is ideal in medical information protection.

V. CONCLUSION

A pseudo random data stream generated from a multi-scroll chaotic attractor is proposed. The multi-scroll chaotic system is composed of continuous-time linear third-order system with feedback of hysteresis-series. The data stream is sampled from the state values at the instance of hysteresis switching. Due to the complicated dynamic behaviors of the hystersis-based chaotic attractor, the generated data stream is highly unpredictable. And the simple model of the multi-scroll chaos makes it easier to be implemented in resource constrained ubiquitous computing environment. The data stream has been implemented in mobile phone with J2ME. The application of this data stream in digital medical image protection for ubiquitous monitoring has also been demonstrated.

Future work will focus on the investigation of the sampled state values from the multi-scroll chaotic systems and to test the randomness of the data stream.

REFERENCES

[1] A. Grami, and B. Schell, "Future Trends in Mobile Commerce: Service offerings, technological advances and security challenges," Proc. of Conf. on Privacy, Security and Trust, Fredericton, 2004, pp.1-14.

[2] Y. Xiao, and H. Chen, Mobile telemedicine, A computing and network perspective. 2008, CRC Press.

[3] S. H. Istepanian, S. Laxminarayan, and C. Pattichis, M-health: emerging mobile health systems, Springer. 2005.

[4] S. Lee, T. Lee, and G. Jin, "An implementation of wireless medical image transmission system on mobile devices," Journal of Medical Systems, vol.32, pp.471–480, 2008.

[5] W. D. Yu, R. Gummadikayala, and S. Mudumbi, "A Web-based wireless mobile system design of security and privacy framework for u-healthcare," 10th IEEE conf. on e-Health Networking, Appl. Serv., pp. 96–101, 2008.

[6] R. Tiwari, S. Buse, and C. Herstatt, "Customer on the Move: Strategic implications of mobile banking for banks and financial enterprises," Proc. of 8th IEEE Conf. on E-Com. Tech., pp. 522–529, 2006.

[7] J. Owens, and B. –H. Anna, Catching the technology wave: mobile phone banking and text-a-payment in the philippines. Chemonics International Inc. 2006.

[8] Mobile banking overview. http://www.mmaglobal.com/mbankingoverview.pdf, 2009.

[9] M. Kumar, and O.P. Sinha, Towards next generation E-government, Computer Society of India, Ed. Bhattacharya J, Hyderabad, pp.294–301, 2007.

[10] K. Roggenkamp, "Development modules to unleash the potential of mobile government," Proc. of 4th European Conf. on e-Government, Zurich, Switzerland, 2004.

[11] H. N. Lee, S. H. Lim, and J. H. Kim, "UMONS: Ubiquitous monitoring system in smart space," IEEE Trans. on Consumer Electronics, vol. 55, no. 3, pp.1056-1064, 2009

[12] N. Kurata, M. Suzuki, S. Saruwatari, and H. Morikawa, "Actual application of ubiquitous structural monitoring system using wireless sensor networks," Proc. International Symposium on Intelligent Signal Processing and Communication. 2006

[13] M. Koji, "Ubiquitous physical monitoring for medical and health care," Journal of the Japan Society of Mechanical Engineers, vol.110, no.1058, pp.38-41, 2007.

[14] Y. D. Lee, D. S. Lee, G. Walia, R. Myllylae, and W. Y. Chung, "Query based duplex vital signal monitoring system using wireless sensor network for ubiquitous healthcare," World Congress on Medical Physics and Biomedical Engineering, pp.396-399, 2006.

[15] R. Wallace, "Addressing the new security challenges of real-time, multimedia, and mobile networks," Nortel Technical Journal, Issue 3, pp.1-6, 2006.

[16] S. T. C. Wong, "A cryptologic based trust centre for medical images," Journal of the American Medical Informatics Association. vol.3, no.6, pp.410-421, 1996.

[17] D. Weerasinghe, M. Rajarajan, and V. Rakocevic, "Device data protection in mobile healthcare applications," Electronic Healthcare, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol.1. Springer Berlin Heidelberg, pp. 82-89, 2009.

[18] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," IEEE Transactions on Vehicular Technology, vol.55, no.4, pp.1373-1384, 2006.

[19] G. Millèrioux, J. Maria, and J. Daafouz, "A connection between chaotic and conventional cryptography," IEEE Transactions on Circuits and Systems-I, 2008, 55(6), pp.1695-1703.

[20] M. E. Yalçın, J. A. K. Suykens, and J. Vandewalle, "True random bit generation from a double-scroll attractor," IEEE Transactions on Circuits and Systems-I, 2004, 51(7), pp.1395-1404.

[21] J. Lü, F. Han, X. Yu and G. Chen. "Generating 3-D multi-scroll chaotic attractors: A hysteresis series switching method," Automatica, vol.40, pp.1677-1687, 2004.

[22] F. Han, X. Yu, Y. Feng, and J. Hu, "On multi-scroll chaotic attractors in hysteresis-based piecewise linear systems," IEEE Transactions on Circuits and Systems-II, 2007, 54(11), pp.1004-1008.

[23] F. Han, J. Hu and K. Xi. "High efficient one time pad key generation for large volume digital data protection," Proc. 5th IEEE Conference on Industrial Electronics and Applications, Taiwan, 2010.

[24] http://en.wikipedia.org/wiki/Hysteresis.

[25] A.N., Mahmood, C. Leckie, and P. Udaya. "An Efficient Clustering Scheme to Exploit Hierarchical Data in Network Traffic Analysis," IEEE Transactions on Knowledge and Data Engineering, 20(6): pp.752-767, 2008.

[26] J. Hu and R. Schyndel . Class Lecture, Topic: "Overview of Mobile Systems." COSC2304, School of Computer Science and Information Technology, RMIT University, Melbourne, Mar, 15, 2010.