Text Encryption and Decryption of DICOM File Header using Jerk Chaotic Attractor

Adisorn Leelasantitham [1] and **Supaporn Kiattisin** [1],

ABSTRACT

This paper presents text encryption and decryption using jerk chaotic attractor. A case study will be tested in DICOM file header for securing patient information. Jerk attractor is a nonlinear mathematical equation and it is a type of chaotic flow which is high chaos and sensitive to initial conditions. Encryption converts the text to binary code and this code is rearranged and resized to small data. Then, the data is embedded and combined with the jerk chaotic system. Finally, the binary code could not be seen before the data encrypted at all. The experimental results show that performance of this algorithm is a high security and a good efficiency. For a case study, DICOM viewers from commercial products cannot open DICOM file which DICOM file header is encrypted by this proposed method. However, it can be opened with decryption of a correct key. Comparisons to other approaches are also presented.

Keywords: text, encryption, decryption, jerk chaos, DICOM file header

1. INTRODUCTION

Digital Imaging and Communications in Medicine (DICOM) [1] has represented fundamental standard in digital medical imaging such as providing all the necessary tools for the diagnostically accurate representation and processing of medical imaging data. Nevertheless, DICOM is not only just an image or file format, but also an all-encompassing data transfer, storage, and display protocol built and designed to cover all functional aspects of digital medical imaging (which is why many view DICOM as a set of standards, rather than a single standard). Another important acronym that seemingly all DICOM companies plug into their names is PACS (Picture Archiving and Communication Systems) [1]. PACS are medical systems (consisting of necessary hardware and software) designed and used to run digital medical imaging. PACS also are directly related to DICOM. Their functionality is DICOM-driven, which ensures their interoperability. For that reason, any PACS device or software comes with its own DICOM Conformance Statement, which is a very important document explaining the extent to which the device supports the DICOM standard. Therefore, PACS [2] bring the DICOM standard to communicate their work.

Nowadays, securing the medical imaging data of the patient needs to consider their information such as their name, birth date, address and picture etc. The main security breach in our DICOM hacking experiment was the readability of the textual part of the *DICOM* file content. For example, we see "SMITHĴOE" in a *DICOM* file, we can easily realize that we deal with a person's name; probably followed by the person's ID and date of birth. If this data is so visible, can it somehow be removed or scrambled? [1]. Therefore, secured *DICOM* file needs to protect the patient information from the hacker. There are many techniques of research papers which have been reported for applications of text security. For example, there have been many algorithms [3-13] such as hashing, RSA, RC4 and statistics etc., but they still have not been more keys and may be hacked by someone. Data compressions [14, 15] have not been more secured for text encryption. Generally, chaotic technique is a high chaos and a high complexity. Chaotic types can be classified into 2 groups i.e. chaotic flow [16-19] consisting of ordinary differential equations (*ODEs*) and chaotic map [20] comprising of logistic equation. Two papers [17, 20] have presented text encryption and decryption whilst other chaotic papers have not proposed them. They can encrypt only ASCII type of characters but they cannot encrypt the Unicode system.

In this paper, text encryption and decryption are presented through the use of jerk chaotic attractor in *DICOM* file header for securing the patient information. This jerk attractor is a non-linear mathematical equation and it is a type of chaotic flow which is high chaos and sensitive to initial conditions. Encryption converts the text to binary code and this code is rearranged and resized to small data. Then, the data is embedded and combined with the jerk chaotic system. Finally, the binary code could not be seen before the data encrypted at all. The experimental results show that performance of this algorithm is a high security and a good efficiency. For a case study, *DICOM* viewers from commercial products cannot open *DICOM* file which *DICOM* file header is encrypted by this proposed method. However, it can be opened with decryption of a correct key. Comparisons to other approaches are also presented.

Manuscript received on August 27, 2013 ; revised on November 21, 2013.

[1] The author is with Technology of Information System Management Program, Faculty of Engineering, Mahidol University, 25/25 Puttamonthon Sai. 4, Salaya, Nakorn Pathom 73170, Thailand, email: adisorn.lee@mahidol.ac.th, tom_kiattisin@hotmail.com

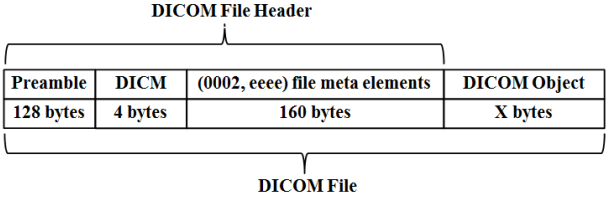


Fig. 1: DICOM file Structure.

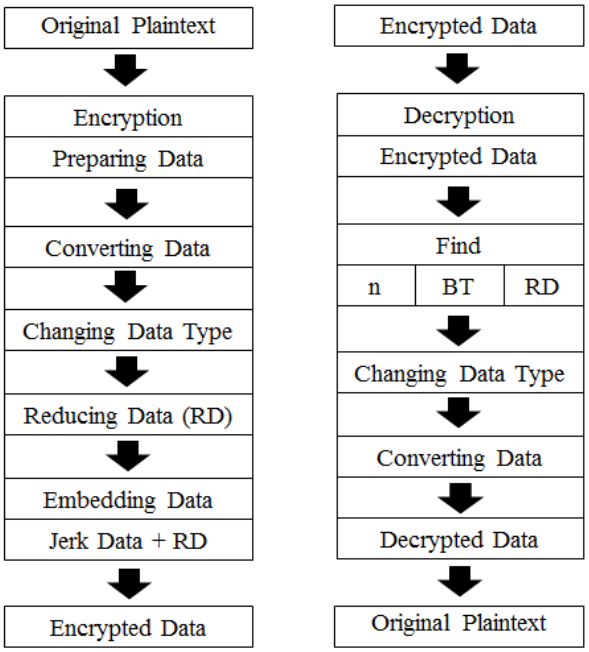


Fig. 2: Proposed methods using jerk attractor for (a) encryption and (b) decryption.

2. DICOM FILE HEADER

DICOM file consists of *DICOM* file header and *DICOM* object, as shown in Fig. 1. The *DICOM* header includes a preamble, a *DICM* prefix, and a pinch of *DICOM* file attributes (file meta elements) [1]. The *DICOM* data object goes right after the 0002 group and stores the actual *DICOM* data. It can be seen from Fig. 1 that total bytes of the *DICOM* file header are approximately at 292 bytes i.e. 128 bytes (preamble), 4 bytes (*DICM* prefix), and 160 bytes (the 0002 group of file meta elements). This research will study to focus on text encryption and decryption in the *DICOM* file header because it is suitable to protect a security of the *DICOM* file.

3. PROPOSED METHODS

3.1 Encrypted/Decrypted Processes

Fig. 2 shows encrypted/decrypted processes using jerk chaos. It can be seen from Fig. 2 that the processes consist of input, encryption, decryption and output. These processes will be described in Sections 3.2 , 3.3 and 3.4

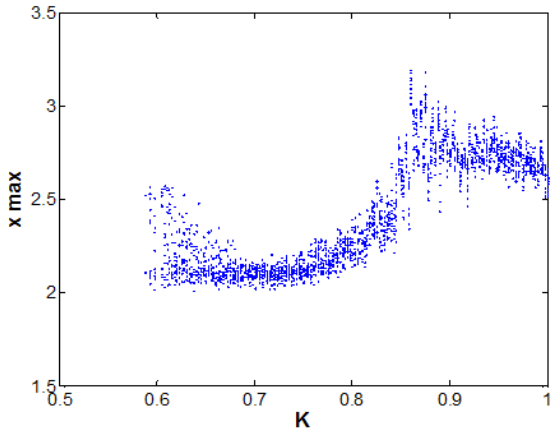


Fig. 3: Bifurcation based on Equs. (2) and (3).

3.2 Jerk Chaotic Attractor

Lorenz [17], Rossler [18] and Chen [19] and chaos are three first-order ordinary differential equations (ODEs) whilst the Sprott's chaotic oscillators [21] is alternatively based on a third-order ODE in a solely-single-coefficient jerk model of the form as

$$\frac{d^3x}{dt^3} + K\frac{d^2x}{dt^2} + \frac{dx}{dt} = G(x) \tag{1}$$

where K is the solely single coefficient and G(x) is a nonlinear component. The term "jerk" comes from the fact that in a mechanical system in which x is the displacement, successive time derivatives of x are velocity, acceleration, and jerk [22]. Rearranging Equ. (1) will be obtained as

$$\frac{d^3x}{dt^3} = -K\frac{d^2x}{dt^2} - \frac{dx}{dt} + G(x) \tag{2}$$

where the non-linear term $G(x)$ is chosen as [20]:

$$G(x) = 1.2x - 4.5\ sgn(x) \tag{3}$$

This chaotic model is a group of chaotic electrical circuit in a term of the non-linear function. It will be used for generating chaotic values to encryption and decryption with the text. Fig. 3 shows bifurcation based on Equs. (2) and (3) of this chaotic model which is described for varying the K to generate the chaos. It can be seen from Fig. 3 that the K can be varied from 0.6 to 1.0 to produce the signal of chaos. This chaotic model (at K = 0.6) has been reported in [21] that Lyaponov exponents (LE), i.e. the highest chaos compared to others, is a maximum value and Kaplan–Yorke dimension (Dky), i.e. the highest complexity compared to others, is also the highest value.

From the Equs. (2) and (3), we choose the value of K = 0.6 and the initial condition of coordinate (x, y, z) = (1, 1, 1) where x, y and z are values in terms of the nonlinear function. Therefore, the values of each

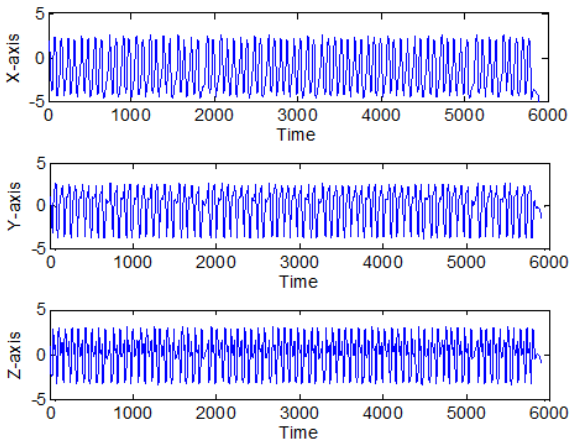


Fig.4: A plot of the generated data (x, y and z axis).

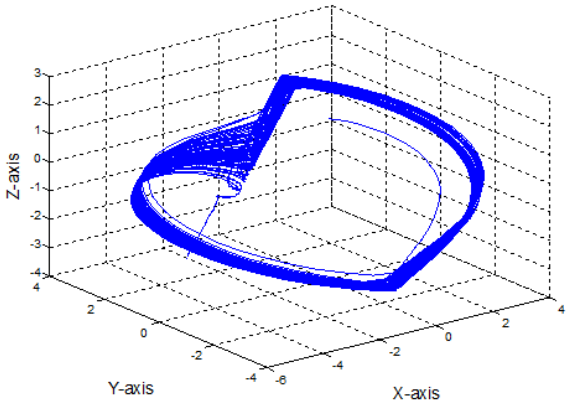


Fig.5: A 3D plot of jerk chaotic attractor.

axis (x, y, z) will be generated approximately at 5,900 data, as shown in Table 1. The ranges of generated data are approximately from -5.886 to 5.886. Fig. 4 shows a plot of the generated data (x, y and z axis) from the Equ. (2). Fig. 5 shows a 3D plot of jerk chaotic equation based on Fig. 4. These generated data will be used for text encryption and decryption in Sections 3.2 and 3.3

3.3 Text Encryption

This method is a new technique for text encryption using the values of C_x, C_y and C_z where C_x, C_y and C_z are the generated data (derived from Section 3.2) of x, y and z axis, respectively. The processes of text encryption can be described as follows:

3.3.1 Encoding Text Data Using C_x

- Preparing a sample of text ” A”, as shown in lines 1 and 2 of Fig 6.
- Converting the text ” A” to Unicode, as shown in line 3 of Fig. 6.
- After that, converting Unicode to binary code which is defined as D_{bin}, as shown in line 4 of Fig. 6.

Table 1: The results of generated data from the Equ. (2).

No.	C_x	C_y	C_z
1	1.000000000000000	1.000000000000000	1.000000000000000
2	1.104197615327810	1.076038054037060	0.526355855619683
3	1.213686553003830	1.106436716159240	0.087670136444942
4	1.324103983560780	1.094779208311830	-0.313462312733505
5	1.431477676586950	1.044831511128210	-0.675448530978549
6	1.532082180804460	0.960772043809871	-0.997720510507891
7	1.622651014497420	0.846627842561239	-1.280431153503880
8	1.700398765679720	0.706220150373578	-1.524427762025630
9	1.763005912012740	0.543167027477590	-1.731228443268550
10	1.808370680309400	0.31061108878779	-1.902798901033650
⋮	⋮	⋮	⋮
5901	-5.886232794590570	-1.480566068244810	-0.919685800046551

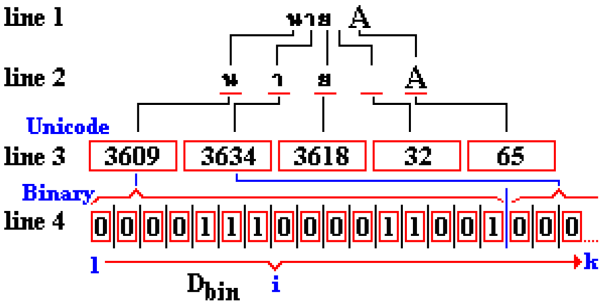


Fig.6: A 3D plot of jerk chaotic attractor.

- Changing a data type from binary (D_{bin}) to double (D_{dou}) for the use of encryption substituted with the C_x, C_y and C_z, as shown in Fig. 7. Numbers of each data (C_x, C_y and C_z) are from $i = 1 \longrightarrow k$ (the position of D_{bin}).
- Reducing the values of D_{dou} by multiplier of 10-n as follow

$$RD = D_{d_{ou}} \times 10^{-n} \tag{4}$$

where n are random positions (1 to 16) of decimal numbers of C_x, as shown in Fig. 8, and RD are the results of $D_{dou} \times 10^{-n}$

- Therefore, the embedded data of text started from $i = 1 \longrightarrow k$ (the position of D_{dou}) can be defined as

$$E_x = RD + C_x \tag{5}$$

where E_x are the values of encoding text data using C_x.

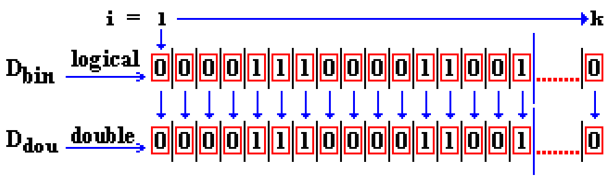


Fig.7: A 3D plot of jerk chaotic attractor.

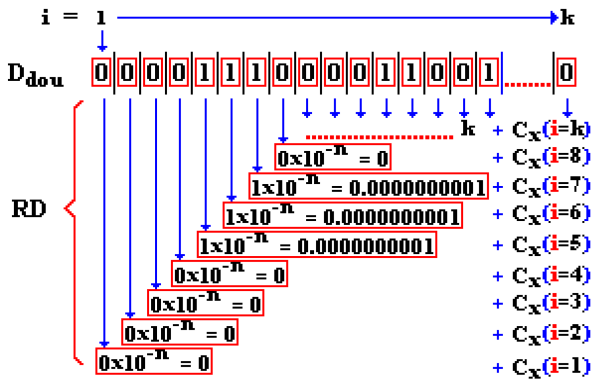


Fig.8:: Reducing the values of D_{dou}.

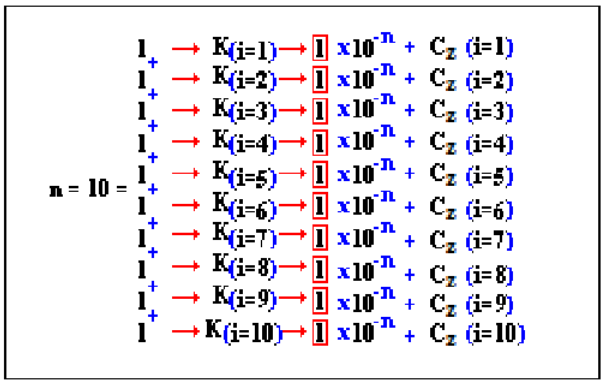


Fig.9:: Encoding the values of n using C_z.

3.3.2 Encoding Length of Text Data Using C_y

For encoding length of text data using C_y, all data D_{bin} are converted to all one which can be defined as

$$BT_{bin} = D_{bin} \bigoplus \overline{D_{bin}} \tag{6}$$

where BT_{bin} are XOR operators of D_{bin} and$\overline{D_{bin}}$. The binary (BT_{bin}) are changed to the double (BT_{dou}). Therefore, the values of E_y in each position (i = 1→k) are

$$E_y = (BT_{dou} \times 10^{-n}) + C_y \tag{7}$$

3.3.3 Encoding Value of n Using C_z

The final step is to encode the values of n using C_z. Therefore, the values of E_z are

$$E_z = (K_{i=1\rightarrow n} \times 10^{-n}) + C_z \tag{8}$$

where K_i are all one and i can be started from $1 \rightarrow n$, as shown in Fig. 9.

3.4 Text Decryption

The values of C_x, C_y and C_z will be again generated from the jerk chaotic attractor with the initial values of x, y, z = 1, 1, 1 approximately at 5,900 times and $A = 0.6$. These values will be used for the processes of text decryption which can be described as follows:

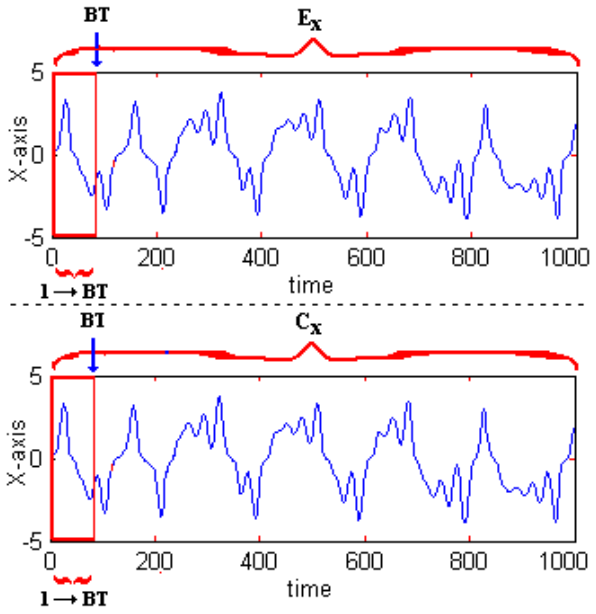


Fig.10:: Selected lengths of both E_x and C_x

3.4.1 Find n

- The values of n can be solved from Equ. (8) as the following equation

$$n = -[\log(E_z - C_z) - \log K] \tag{9}$$

3.4.2 Find BT

- The values of BT_{dou} in each position (i = 1→k) can be solved from Equ. (7) as the following equation

$$BT_{dou} = \frac{E_y - C_y}{10^{-n}} \tag{10}$$

- The results of Equ. (10) in each position (i = 1→k) can be calculated for total length (BT) of text decryption as the following equation

$$BT = \sum_{i=1}^{k} BT_{dou} \tag{11}$$

Fig. 10 shows selected lengths of the data E_x and C_x. It can be seen from Fig. 10 that the red block is the selected lengths from all of the data of both E_x and C_x using the starting values from 1 to BT of Equ. (11).

3.4.3 Find RD

- The values of RD and D_{dou} in each position using $i = 1 \rightarrow BT$ can be solved from Equs. (5) and (11) as the following equations

$$RD = E_{x(i-1\rightarrow BT)} - C_{x(i=1\rightarrow BT))} \tag{12}$$

$$D_{dou} = \frac{RD}{10^{-n}} \tag{13}$$

- The data type of Equ. (13) will be changed to the data type of binary (D_{bin}) or logical values, as shown in Fig. 11.

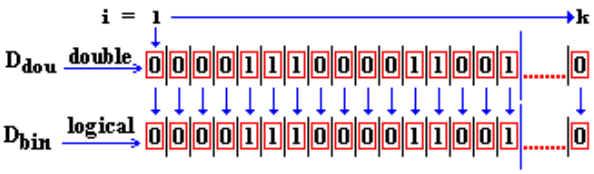


Fig.11:: Selected lengths of both E_x and C_x.

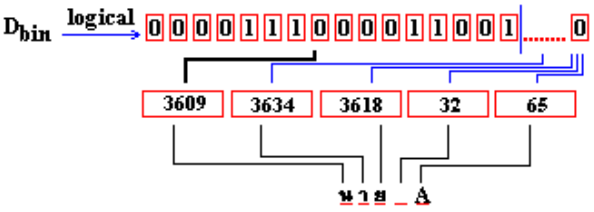


Fig. 12:: The data type of D_{bin} converted to the characters of the Unicode system.

• Therefore, numbers of characters for the Unicode system can be obtained as

$$CU = \frac{D_{bin}}{16} \tag{14}$$

Fig. 12 shows the data type of D_{bin} converted to the characters of the Unicode system. It can be seen from Fig. 12 that the sample of text ” A” is decrypted.

4. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

4.1 Experimental Results

Table 2 shows numbers of characters for text encryption and decryption. It can be seen from Table 2 that the proposed method can encrypt and decrypt all of the text among numbers of characters (1 to 368), but it cannot encrypt and decrypt them in the case of more than 368 characters. However, we can improve this system to increase the higher characters using adjusting the initial values of the commonly distributed coefficient (A) and coordinates (x, y, z). Fig. 13 shows sample results of encryption and decryption in Thai text as ” A”. Figs. 13 (a), (b) and (c) show the results of input, encryption and decryption, respectively. As mentioned earlier in Section 2. the proposed method can use text encryption and decryption in all DICOM file header of 292 bytes. It is enough to encrypt them because the maximum characters can use up to 368, as shown in Table 2. For the results in this study, DICOM viewers from commercial products cannot open the DICOM file which is encrypted by this proposed method. However, it can be opened with decryption of a correct key.

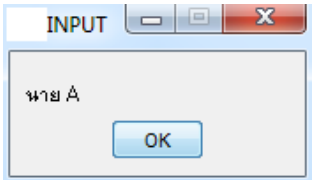
4.2 Security Analysis

4.2.1 Key Space Analysis

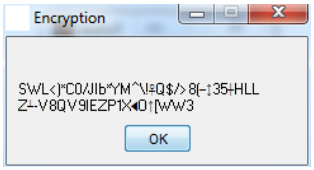
Numbers of keys can be considered as follows: the constant values (from Equ. (3)) of 1.2 and -4.5, the values of x, y, z and K. Then, there have the total keys of 6 which each key consists of 16 bits. The total bits are 96 (or 6×16). Therefore, numbers of key space for text encryption are high to 2^{96} digits which can be applied for the use (56 bits or 64 bits) in Data Encryption Standard (*DES*) [10].

Table 2:: Numbers of Characters for Encryption and Decryption.

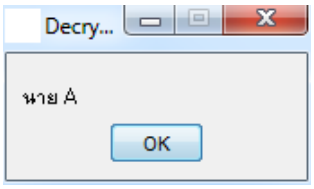
Numbers of Characters for Encryption	Initial Values of (x,y,z)	Decryption (Passed or Fail)
1-100	(1,1,1)	Passed
100-200	(1,1,1)	Passed
200-300	(1,1,1)	Passed
300-368	(1,1,1)	Passed
369 up	(1,1,1)	Fail



(a)



(b)



(c)

Fig. 13:: 13 Sample results of Thai text “ A” for (a) input, (b) encryption and (c) decryption.

4.2.2 Key Sensitivity

Key sensitivity is a test for varying the key space through the use of changing the decimal digits. If the resulting from the decryption is a correct text, then it means that the decrypted key is a correct key. However, if it is not a correct text, then the decrypted key is not a correct key. For example, if the input key is $(x, y, z) = (1.0000001, 1, 1)$, the decimal position of x equal to 7 digits, then ” A” will be encrypted by this input key. Thus, the resulting of encryption is shown in Fig. 14 which is different from Fig. 13 using the input key of $(x, y, z) = (1, 1, 1)$. If the key of decryption is $(x, y, z) = (1.0000001, 1, 1)$, then the text will be decrypted for a correction. Nevertheless, if the key of decryption is $(x, y, z) = (1.00000001, 1, 1)$, the decimal position of x equal to 8 digits, then

Table 3:: Comparisons of performances between this paper and other chaotic techniques (a) chaotic flow and (b) chaotic map, ✓ = Yes, x = No.

Chaotic Techniques → Performances ↓	Chaotic Types					
	(a) Chaotic Flow					(b) Chaotic Map
	This paper	Jerk [16]	Lorenz [17]	Rossler [18]	Chen and Lu [19]	Logistic Map [20]
Terms in equation	5	5	7	7	6	x
ODEs	1	1	3	3	3	x
Components of Circuits	Very Little	Little	Little	Little	Little	Very Large
Time of Calculation	Very Fast	Fast	Fast	Fast	Fast	Depended on CPU
LE>0	✓	✓	✓	✓	✓	x(Recurrence Model)
Dky<3	✓	✓	✓	✓	✓	x(Recurrence Model)
Text Encryption/Decryption	✓	x	✓	x	x	✓
Type of Characters	Unicode & ASCII	x	ASCII	x	x	ASCII
Key Space	2^{96}digits	x	x	x	x	x
Key Sensitivity	High	x	x	x	x	x
Power Spectrum	✓	x	x	x	x	x
DES(56 bits or 64 bits)	✓	x	x	x	x	x

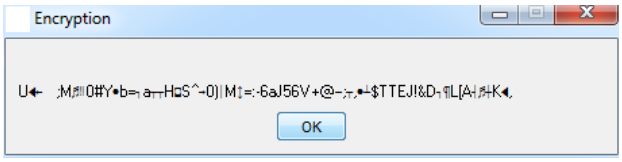
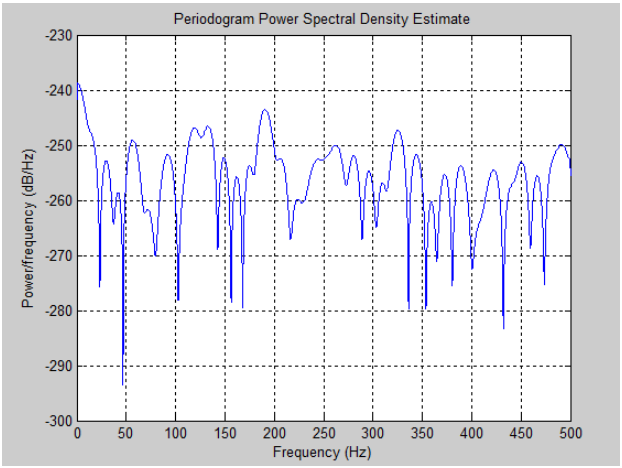


Fig. 14:: Encryption results of Thai text ” A” using the input key of $(x, y, z) = (1.0000001, 1, 1)$.

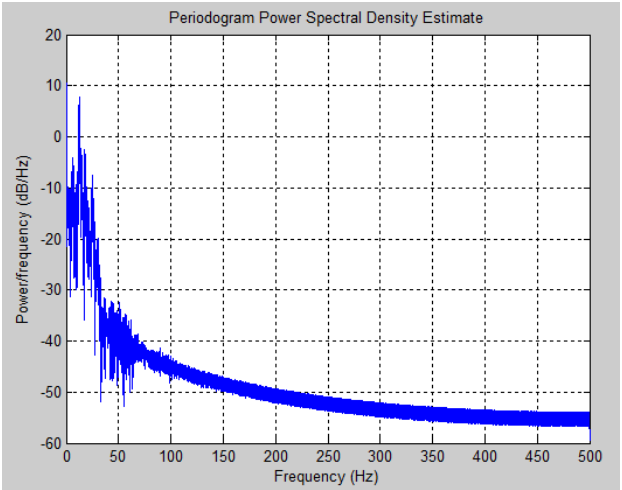
it cannot decrypt the text. Therefore, this proposed method using jerk chaotic attractor presents information security for encrypting and decrypting the text because it is a high sensitivity to change the input key.

4.2.3 Power Spectrum Analysis

Power spectrum analysis leads to depict a signal graph in terms of text patterns considering the encryption of before and after. Figs. 15 (a) and (b) show power spectrum of before and after, respectively, encryption in the text ” A” based on Equs. (4) and (5), respectively. It can be seen from Fig. 15 (b) that the power of encrypted text is approximately at 0-40 dB/Hz, higher than the power of Fig. 15 (a), and it also is a high complexity.



(a)



(b)

Fig. 15:: Power spectrum plots of Thai text ” A” for (a) before encryption and (b) after encryption.

5. COMPARISONS

In Table 3, the performances of this paper are particularly compared to those of existing (a) chaotic flow and (b) chaotic map in terms of numbers of terms in equation, numbers of *ODE* equation, components of circuits, time of calculation, $LE > 0$, $Dky < 3$, text encryption and decryption, type of characters, key space, key sensitivity, power spectrum and *DES* (56 bits or 64 bits).

It can be seen from Table 3 that this paper offers much better performances than other chaotic techniques. This jerk attractor is a type of chaotic flow which is high chaos and sensitive to initial conditions. For example, numbers of terms in equation is low at 5 terms. Numbers of *ODE* equation is lowest at 1. Components of circuits are very little. Time of calculation is very fast because of low terms and ODE equation. It has a high chaos ($LE > 0$) and it has a high complexity ($Dky < 3$). It can be applied for text encryption and decryption based on Unicode system and ASCII. Key space is equal to 2^{96} digits. Key sensitivity is high. It has an analysis of the power spectrum. It also can be supported for *DES* (56 bits or 64 bits).

In addition, only two papers have proposed text encryption and decryption using chaotic Lorenz [17] and logistic map [20]. However, their papers have not been reported for others performances e.g. key space, key sensitivity, power spectrum and *DES* (56 bits or 64 bits). They can encrypt only ASCII types of characters but they cannot encrypt the Unicode system. This work therefore offers not only much better performances compared to other chaotic techniques, but also a potential alternative to develop practical applications for securing the *DICOM* information in the future.

6. CONCLUSION

This paper has presented the text encryption and decryption using jerk chaotic attractor in *DICOM* file header for securing the patient information. This jerk attractor is a nonlinear mathematical equation and it is a type of chaotic flow which is high chaos and sensitive to initial conditions. The encryption converts the text to binary code and this code is rearranged and resized to small data. Then, the data is embedded and combined with the jerk chaotic system. Finally, the binary code could not be seen before the data encrypted at all. The experimental results show that performance of this algorithm has been the high security and the good efficiency. For a case study, *DICOM* viewers from commercial products cannot open *DICOM* file which *DICOM* file header is encrypted by this proposed method. However, it can be opened with decryption of a correct key. Comparisons to other approaches have been also presented.

ACKNOWLEDGEMENTS

The authors are grateful to Faculty of Engineering, Mahidol University for the research scholarship, and to Mr. Prawit Laosomboon for his useful help in this work. They also would like to thank Assoc. Prof. Banlue Srisuchinwong and Asst. Prof. Wimol San-Um for their useful suggestions.

References

[1] Oleg S. Pianykh, "Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide.", *Springer-Verlag Berlin Heidelberg*, 2008.

[2] P. Suapang, S. Yimman and K. Dejhan, "Medical Image Processing and Radiology Information System.", *International Journal of Applied Biomedical Engineering (IJABME)*, vol. 5, pp. 61-70, 2012.

[3] Goldwasser, Shafi Micali, Silvio Tong, Po,"Why and how to establish a private code on a public network.", *Foundations of Computer Science*, pp. 134–144, 1982.

[4] J. Katajainen and T. Raita, "An Approximation Algorithm for Space-optimal Encoding of a Text.", *The Computer Journal*, pp. 228-237, 1989.

[5] Mantin and A. Shamir., "Weaknesses in the key scheduling algorithm of RC4.", *Lecture Notes in Computer Science Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, vol. 2259, pp. 1 - 24, 2001.

[6] Bao-Chyuan Guan,Ray-I Chang, Yung Chung Wei, Chia-Ling Hu, Yu-Lin Chiu, "An encryption scheme for large Chinese texts.", *Security Technology*, pp.564–568, 2003.

[7] Sreelaja, N.K.; Vijayalakshmi Pai, G.A, "Swarm intelligence based key generation for text encryption in cellular networks.", *Communication Systems Software and Middleware and Workshops*, pp.622 – 629, 2008.

[8] Suli Wu; Xiaofei Yi, "Text Encryption Algorithm Based Cyclic Shift.", *E-Business and E-Government (ICEE)*, pp. 3483–3486, 2010.

[9] Singh, K. and Ghosh Samaddar, S., "Selective encryption technique in RSA based singular cubic curve with AVK for text based documents: Enhancement of Koyama approach.", *2010 International Conference on Networking and Information Technology (ICNIT)*, pp. 343–349, 2010.

[10] Wen-Xiang Zhang, Si-You Xiao and Yi Zhang, "Research on Image-Text Encryption Techniques in Mobile Communications.", *The 2010 Second WRI Global Congress on Intelligent Systems (GCIS)*, vol. 2, pp. 115 – 118, 2010.

[11] L. Moltedo, A. Noferini, "An Implementation of 7-bit Character Encoding for Standard Computer Graphics Environments.", *The Computer Journal* ,pp.429-436, 1990.

[12] B. E. S. Rinza, D. A. B. Zavala, A. C. Chavez, "De-Encryption of a Text in Spanish Using Prob-

ability and Statistics.", *Electronics, Communications and Computers*, pp. 75–77, 2008.
[13] C. Rupa, P. S. Avadhani, "Message Encryption Scheme Using Cheating Text.", *Computational Intelligence and Software Engineering*, pp. 1-4, 2009.
[14] R. W. Franceschini, A. Mukherjee, "Data compression using encrypted text.", *Data Compression Conference*, 1996.
[15] H. Kruse, A. Mukherjee,"Data compression using text encryption.", *Data Compression Conference*, 1997.
[16] B. Srisuchinwong,"Chaos in a Fractional-Order Jerk Model using Tanh Nonlinearity.", *Proceedings of the 2nd Chaotic Modeling & Simulation International Conference (CHAOS 2009), Chania, Crete, Greece*, 1-5 June, pp. 8, 2009.
[17] Yuan Ji, Changyun Wen, Zhengguo Li, "A Practical Chaotic Secure Communication Scheme Based on Lorenz Model.", *IEEE International Conference on Industrial Informatics*, pp. 576–580, 2006.
[18] O. E. Rössler, "An equation for continuous chaos.", *Physics Letters A*, 57 (5), pp. 397-398, 1976.
[19] J. Lu, G. Chen, S. Zhang, "The Compound Structure of a new Chaotic Attractor.", *Chaos, Solitons and Fractals*, 14, pp. 669-672, 2002.
[20] Ching-Kun Chen, Chun-Liang Lin, "Text encryption using ECG signals with chaotic Logistic map.", *Industrial Electronics and Applications (ICIEA)*, pp. 1741-1746, 2010.
[21] J. C. Sprott, "A New Class of Chaotic Circuit.", *Physics Letters A*, vol. 266, pp. 19-23, 2000.
[22] S. H. Schot, "The time rate of change of acceleration.", *Am. J. Phys.*, vol. 46, pp. 1090-1094, 1978.

Adisorn Leelasantitham received the B.Eng. degree in Electronics and Telecommunications and the M.Eng. degree in Electrical Engineering from King Mongkut's University of Technology Thonburi (KMUTT), Thailand, in 1997 and 1999, respectively. He received his Ph.D. degree in Electrical Engineering from Sirindhorn International Institute of Technology (SIIT), Thammasat University, Thailand, in 2005. He is currently the Assistant Professor in Technology of Information System Management Program, Faculty of Engineering, Mahidol University, Thailand. His research interests include analog circuits, image processing, medical images, computer graphics, AI, neural networks, microcontrollers, embedded systems, robotics and applications of chaos systems.

Supaporn Kiattisin received B.Eng. in Computer Engineering from Chiangmai University in 1995, M.Eng. in Electrical Engineering and Ph.D. in Electrical and Computer Engineering from King Mongkuts University of Technology Thonburi (KMUTT), Bangkok, Thailand. She currently works at Technology of Information System Management Program, Faculty of Engineering, Mahidol University, Thailand. Her research interests include medical imaging, computer vision and modeling. She is member of TESA, ThaiBME, IEICE and IEEE.