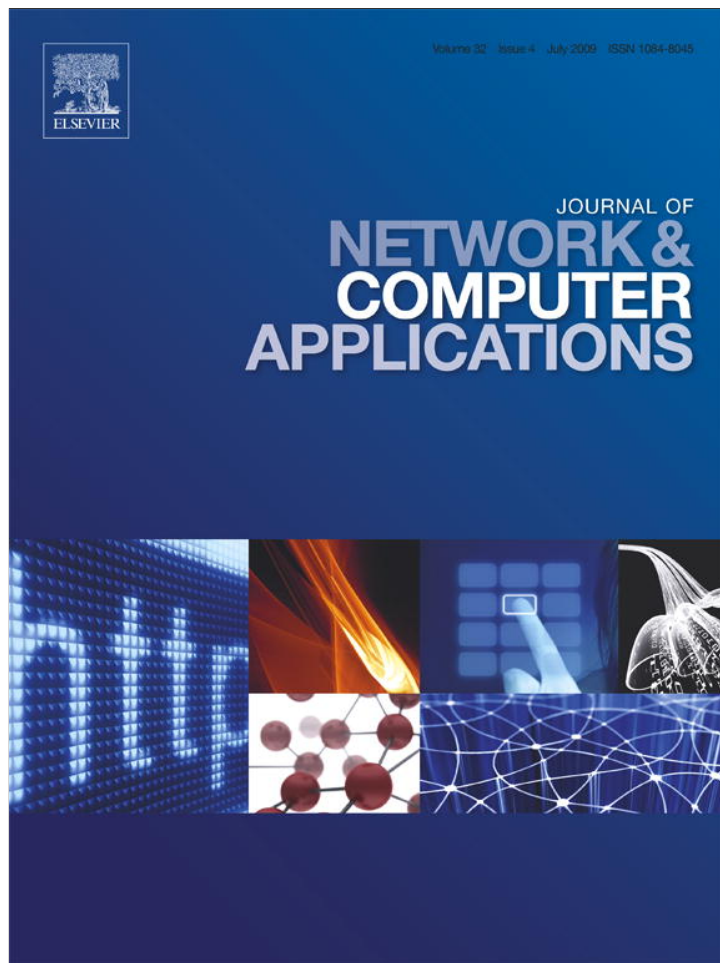


Provided for non-commercial research and education use.
Not for reproduction, distribution or commercial use.



This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier's archiving and manuscript policies are encouraged to visit:

<http://www.elsevier.com/copyright>



Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A pixel-based scrambling scheme for digital medical images protection

Jiankun Hu*, Fengling Han

RMIT University, Melbourne 3001, Australia

ARTICLE INFO

Article history:

Received 30 May 2008

Received in revised form

5 February 2009

Accepted 26 February 2009

Keywords:

Chaos

Digital medical images protection

Image scrambling

True random number sequences

ABSTRACT

This paper proposes a novel pixel-based scrambling scheme to protect, in an efficient and secure way, the distribution of digital medical images. To provide an efficient encryption of a large volume of digital medical images, the proposed system uses simple pixel level XOR operation for image scrambling in an innovative way such that structural parameters of the encryption scheme have become a part of the cryptographic key. The cryptographic key of this operation is a true random number sequence generated from multi-scroll chaotic attractors.

Cryptanalysis is provided. Simulation experiment has also validated the effectiveness of the proposed system.

© 2009 Elsevier Ltd. All rights reserved.

1. Introduction

The need for distribution of digital medical images over networks has become an essential part of everyday life in medical systems. There are two main factors behind this phenomenon. *Factor 1* is that digital medical image records provide better tools for diagnosis, treatment, and surgery than what conventional film-screening-based mechanisms can offer. Hence the use of digital medical image is encouraged. There are many applications where the deployment of digital medical image archiving, transmission and processing can offer better medical services that conventional non-digital medical images fail to deliver. One typical example is breast cancer detection. Statistics indicates that breast cancer has become the fourth common cause of death among women in the United States (Boring et al., 1992; Zhou et al., 2001). The most effective breast cancer control approach relies on early detection via massive screening with periodic mammography and physical examination. However, the most widely used film-screening mammography systems have several technical limitations that can reduce breast cancer diagnostic accuracy. Digital mammography can resolve these problems and also provide more fine features such as contrast enhancement, digital archiving, and computer-aided diagnosis that help increase the diagnostic accuracy significantly (Zhou et al., 2001). *Factor 2* is that medical examination site, digital medical image capturing site and digital medical image storage site are often geographically separated where medical data flow over networks is a must.

To make good use of the resources, the trend in sharing digital medical images is rapidly increasing in the healthcare community (Montagnat et al., 2004), which is further imposing an even greater demand for the distribution of digital medical images over public networks. A typical such example is telemedicine.

Telemedicine is emerging as a powerful technological platform where distributed medication resources especially medical expertise from global gold medallists can be utilized anytime anywhere. In tele-mammography, for instance, it uses full field digital mammography (FFDM) units at the examination site in combination with the expert centre (Lou et al., 1997). Real-time tele-mammography examinations are being conducted and real-time digital medical images being transmitted via WAN and are diagnosed with the help of distributed medical experts.

Medical applications often deal with patients' data that are confidential and should only be accessible to authorized persons (Formazin et al., 2008). While some patients are unconcerned about confidentiality, there are others for whom breach of confidentiality could cause extreme embarrassment, humiliation, and even loss of employment. Therefore, for legal and ethical reasons, there is an urgent need to protect the confidentiality of patients' records stored as well as of those of any kind transmitted (Norcen et al., 2003; Dickson et al., 2007).

Picture Archiving and Communication Systems (PACS) as well as Digital Imaging and Communications in Medicine (DICOM) provide the current medical image transport and storage standards. Security mechanism (cryptosystems) deployed in existing digital medical image systems is almost exclusively based on the conventional cryptography which has been designed to protect textual data. Digital medical images, such as the magnetic resonance images (MRIs), computed tomography (CT),

* Corresponding author. Tel.: +61 3 99259793; fax: +61 3 9662 1617.
E-mail address: jiankun@cs.rmit.edu.au (J. Hu).

are data types that require enormous storage capacity or transmission bandwidth if treated as textual data. It ranges from less than a megabyte to around 30 megabytes for different modalities (Rahman et al., 2004). To reduce the high cost of encrypting large amount of digital medical image data, one popular method for confidentiality protection is to embed patients' identification information in medical images (Coatrieux et al., 2008). The latest DICOM standard defines the image format and a peer-to-peer network transport protocol. Each DICOM formatted image includes a small size header file containing patients' sensitive information, such as name, birth date, home address, gender, and history (textual data), and a very large image pixel data file. If the textual data do not appear on medical images, it would be difficult to link the images with the corresponding patients in some circumstance. Security filtering the textual data is one option to protect medical images (Wang, 2001). Steganography and watermarking technologies were used to embed patients' information in digital medical images (Chiarelli, 2004; Coatrieux et al., 2008). The hidden data (text) is encrypted into a medical image with a key. Another popular method to protect confidentiality of digital medical image is selective encryption, which trades off security for computational complexity. Selective encryption algorithm based on Advanced Encryption Standard (AES) has been proposed, in which the entire image is divided into some small blocks, encryption uses identical key for all blocks (Norcen et al., 2003; Snyder, 2003). Consequently, if there are identical plain blocks, these data produce identical ciphertext blocks, as shown in Fig. 1, which would provide useful information to the attackers. Although other modes such as Cipher Block Chaining (CBC) can reduce the effect of this deficiency, it is not always trivial in narrowing down selective regions into a small part to enjoy the benefit of encryption efficiency while make sure any malicious alterations on non-selective part is damage free.

Most recent medical-imaging devices produce 3D images which can produce the amount of image data up to GB level. A standard 3D Computed Tomography scan (CTscan) of magnetic resonance image represents tens to hundreds of MB of data (National Digital Medical Archive, Inc., 2008). In some cases, a full effective digital medical image or a large part of the digital medical image needs to be protected. Typical examples are long bone panoramas from fluoroscopic X-ray images (Ziv and Leo, 2004), and image-based diagnosis of Alzheimer-type Dementia (Kodama et al., 2002). It is desirable to develop encryption algorithms for efficient encryption of large digital medical images for real-time environment. Much effort is needed to strike a better balance of cryptographic encryption strength and efficiency for the distribution of digital medical images over networks. This will be the focus of this paper. For issues related to other aspects of the

security such as authentication, non-repudiations, etc., interested readers are referred to Hu et al. (2008) and references therein.

In this paper, we present a pixel-based scrambling scheme, which provides an efficient and strong security mechanism for the protection of digital medical images. In this scheme, a novel digital medical image scrambling algorithm (ISA) based on the simple XOR operation is proposed. To provide a good cryptographic strength, the scrambling key is a true random number (TRN) sequence that is derived from the multi-scroll chaotic attractors. Although the proposed scrambling scheme is a linear operation, its structure is not fixed and instead it has become an integral part of the cryptographic key, which makes linear cryptanalysis attack and differential cryptanalysis attack infeasible. Statistical cryptanalysis and simulation experiment have been provided to validate the proposed scheme. Experiment has shown that the proposed image encryption scheme is more than 100 times in efficiency than that of the AES scheme, which renders it a suitable candidate for real-time encryption of digital medical images.

The remaining of this paper is organized as follows. Section 2 introduces the proposed pixel-based scrambling algorithm. Section 3 presents the evaluation of this image scramble scheme. Conclusions are drawn in Section 4.

2. An efficient and secure pixel-based images scrambling scheme

It is known that the most promising algorithm for the protection of digital medical images is to analyze the unique properties of digital medical image, make full use of these properties and search for high security algorithms that cause minimal computational overhead (Yang et al., 2004). In this section, an efficient and secure pixel-based images scrambling scheme is proposed. The efficiency of the digital medical image scrambling is achieved by the simplicity of the XOR operation. The true random scrambling key derived from the chaos cryptography provides the cryptographic security strength of this scrambling scheme.

2.1. Image scrambling with simple XOR operations

The XOR, denoted as \oplus , is the binary exclusive which is an elemental computer operation. It could be implemented easily by both software and hardware, and is less computational demanding (Dawson and Nielsen, 1996).

For a grey level $m \times n$ (row number m , column number n) two-dimensional image shown in Fig. 2a, the grey level value of the corresponding pixel at (x, y) can be represented as $g = f_{m,n}(x, y)$. To convert this l -bit size $m \times n$ grey level image (bitmap) into $m \times (l \times n)$ binary image (monochromatic), as shown in Fig. 2b, each grey level value can be represented by a l -bit binary number.

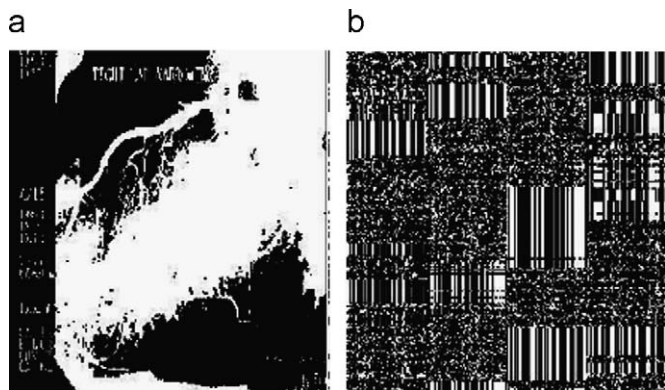


Fig. 1. (a) Digital medical image and (b) encrypted with AES (Norcen et al., 2003).

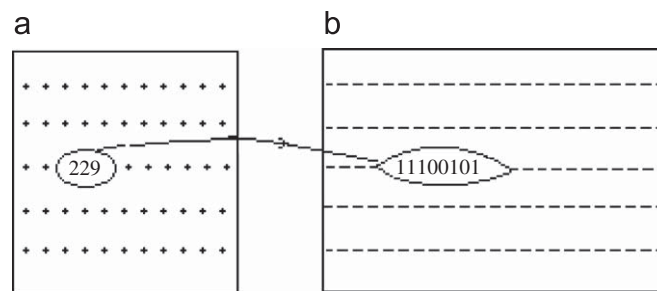


Fig. 2. (a) Raw $[m, n]$ image with eight grey level values and (b) converted $[m, n \times 8]$ binary image.

This $m \times (l \times n)$ binary image Fig. 2b can be scrambled by the following image scrambling algorithm. To begin with, following definitions are made:

Row-round scrambling (RRS): Randomly choose p rows as seed rows from 1 to m rows of the raw image. These seed rows are represented in binary values as $[b_{ij}(i = 1, \dots, p; j = 1, \dots, n \times l)]$. Then randomly select a seed row k from these p seed rows, seed row block, to perform XOR operation bitwise with any other rows of the binary image (except the seed row block) which generates:

$$b_{i,j} = b_{i,j} \oplus b_{k,j} (i = 1, \dots, m, (i \neq k, k = 1, \dots, p), j = 1, \dots, n \times l). \quad (1)$$

One RRS ends when all chosen p seed rows have been performed according to Eq. (1). Because the XOR operation is commutable, the order of selected seed rows in the XOR operation does not affect the final result.

Column-round scrambling (CRS): Similar to the definition of RRS, we can define seed columns and construct a column-round image scrambling by substituting rows with columns.

One round of scrambling (ORS): A mix of RRSs and CRSs for one round.

ISA algorithm

Step 1: Given a greyscale medical image, convert it into its corresponding binary image.

Step 2: Determine following values: (i) maximum number of ORSs needed. Our extensive experiments show that 30 is a good choice; (ii) number of RRSs and number of CRSs within each ORS; (iii) order of performing RRSs and CRSs within each ORS and (iv) seed rows within each RRS and seed columns within each CRS. Values in (ii)–(iv) are actually derived from a cryptographic key which is a random number. In the next section a method is proposed to generate such random numbers.

Step 3: Complete the image scrambling by running all ORSs defined in the step 2.

Due to the randomness of the XOR operation on a bit level, the grey level values of the pixel level image tend to be randomly and evenly distributed which renders it infeasible to retrieve raw image features without the cryptographic key. The raw image can be fully recovered by performing the XOR operation in the reverse order with the help of the cryptographic key.

An illustrative example is provided in the following. Suppose that we have a 6×6 binary image data. The RRS process is shown in Fig. 3. In Fig. 3a, the third and fifth rows are selected as seed block (then $p = 2$) to scramble the data; Fig. 3b is obtained by XOR the seed block with Fig. 3a from the beginning to the end while keep the rows in seed block (third and fifth rows) unchanged.

To recover the original data in Fig. 3a, one should perform the same XOR operation in the reverse order of the scrambling process.

2.2. Generating true random scrambling key from multi-scroll chaos

It is well known in Cryptography community that encryption schemes are not taken as a secret while a cryptographic key is.

1 0 0 1 1 1	\oplus row3 \oplus row5	\rightarrow	0 1 0 1 0 0
0 1 1 1 0 0	\oplus row3 \oplus row5	\rightarrow	1 0 1 1 1 1
0 0 1 1 1 1	unchanged	\rightarrow	0 0 1 1 1 1
1 1 0 0 0 1	\oplus row3 \oplus row5	\rightarrow	0 0 0 0 1 0
1 1 1 1 0 0	unchanged	\rightarrow	1 1 1 1 0 0
1 1 1 0 0 0	\oplus row3 \oplus row5	\rightarrow	0 0 1 0 1 1

Fig. 3. Pixel wise XOR with the selected row number being a key: (a) original binary image, rows 3 and 5 are selected as key and (b) scrambled image after one RRS operation.

Therefore, the strength of the cryptographic key is essential in any cryptosystems. A true random cryptographic key will force attackers enter an exhaustive search mode within the key space which will end up with a computational infeasible status when the key space is large enough. In this section, a true random cryptographic key for our ISA digital medical image scrambling algorithm proposed in the previous subsection is extracted from the multi-scroll chaos.

Chaotic systems are sensitive to initial conditions, and this sensitivity causes long-term unpredictability (Chen et al., 2004). Chaos-based medical image encryption has been reported (Ashtiyani et al., 2008). A most encouraging application of chaotic signals in engineering is its use as a source for random number generator (RNG) (Yalçın et al., 2004). True random bit generation for cryptographic applications have been proposed (Yalçın et al., 2004; Pareschi et al., 2006). In their work, true random numbers are proposed to be generated from double-scroll chaotic attractors, in which the scrolls are discretized and coded in space instead of in time. Sampling the chaotic signal in space gives an irregular sampling of the signal in time. Therefore, it becomes very hard to make a prediction for an opponent in cryptography (Yalçın et al., 2004).

More scrolls would produce higher complex dynamic behaviours. More complex attractors may further improve unpredictability (Yalçın et al., 2004). In our previous work, multi-scroll chaotic attractors have been found (Han et al., 2003, 2005, 2007). In the following, a method is proposed to generate TRNs from these multi-scroll chaotic attractors.

The $(p+1) \times (q+1)$ scrolls chaotic attractors are generated by a continuous time linear system with a feedback of hysteresis series, which can be described as

$$\begin{cases} \dot{x} = y - h(x, q), \\ \dot{y} = -ax + by + ah(x, p), \end{cases} \quad (2)$$

where x and y are two state variables, a and b are two parameters. And we have

$$h(x, n) = \sum_{i=1}^n h_i(x), \quad (3)$$

where $h(x, n)$ represents the output of a hysteresis series as shown in Fig. 4a (Han et al., 2003), the input of which is a state variable, and n is the number of hysteresis.

When $a = 1$, $b = 0.125$, $p = 6$, $q = 4$, system (3) has $(p+1) \times (q+1)$ equilibrium points, which are given by

$$O_{xy} = [(i, j) | i = 0, 1, \dots, p; j = 0, 1, \dots, q]. \quad (4)$$

Firstly, the state space is partitioned into $(p+1) \times (q+1)$ sub-spaces. Two groups of true random sequences are extracted from two state variables x and y , respectively, which is represented as T_1 and T_2 . For each group, the points where trajectories intersect with the switching lines are recorded, those points switched by their upper switching lines are recorded as 1, and those switched by their lower switching lines are 0. This process is illustrated in Fig. 4.

In Fig. 4, the systems trajectories around any equilibrium point are evolving clockwise and will be switched by the output of hysteresis series in either horizontal or vertical direction depending on the initial values when trajectory landed on the basin of attraction of corresponding equilibrium point. In each direction, the trajectory will be switched by either its upper or lower switching lines. Fig. 4a shows that the trajectory is switched by its lower switching lines vertically; this will produce a number 0 in T_2 . Fig. 4b shows the trajectory is switched by its upper switching lines vertically; this will produce a number 1 in T_2 . Fig. 4c shows the trajectory is switched by its lower switching lines horizontally

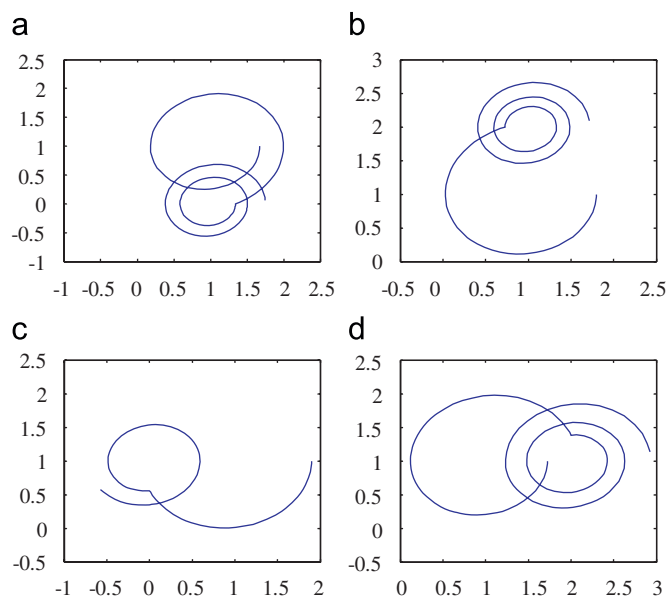


Fig. 4. Collection of true random number sequences: (a) $b_i = 0$, (b) $b_i = 1$, (c) $b_i = 0$, and (d) $b_i = 1$.

and it will produce a number 0 in T_1 . And Fig. 4d shows the trajectory is switched by their upper switching lines horizontally and it will produce a number 1 in T_1 .

From Fig. 4, one can see that there are four cases that the trajectory would be switched for the two-dimensional multi-scroll attractors when it evolves around any equilibrium point except those outside ones, $O_{xy} = [(i,j)|i = 0 \text{ and } p; j = 0, 1, \dots, q]$, and $O_{xy} = [(i,j)|i = 0, 1, \dots, p; j = 0 \text{ and } q]$. Which case would happen depends on the initial conditions when trajectory landed on the basin of attraction of the corresponding equilibrium point. For the trajectories around the outside of equilibriums, there are three possibilities for trajectories evolve; and for the trajectories around corner equilibrium point, O_{00} , O_{0p} , O_{p0} and O_{pq} , there are two possibilities for trajectory evolve.

Statistic tests determine whether the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit. There are many practical measures of randomness for a binary sequence, repetitions of '01'. The true randomness of the double-scroll attractor has passed a large number of statistical tests. More complex attractors such as n -scrolls or scroll grid attractors can further improve unpredictability (Yalçın et al., 2004). The multi-scroll attractors (scroll grid attractor) demonstrate more complex dynamical behaviour than that of double-scroll attractors. Therefore, both T_1 and T_2 are true random number sequences.

In order to guarantee collecting the random bit sequence, two thresholds, c_1 and c_2 , are defined for extract binary values from continuous time signal according to Yalçın et al. (2004). This issue is not the focus of this paper.

2.3. Discussions

In cryptography, an encryption algorithm is usually assumed to be known to the opponents. Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. The encryption key that determines the procedure of XOR operation in the proposed ISA algorithm is a true random number sequence.

In addition to the randomness, the security level of an encryption algorithm is also measured by the size of the key

space. The larger the size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. As the proposed image scrambling algorithm is based on the row-round and column-round XOR operation, the size of the key space is increased exponentially with the number of rounds. Thus, the original images could be thoroughly scrambled. More in-depth analysis on this is provided in the remaining Section 3. With the increase of the number of XOR operations, the security level of the encrypted image could be greatly enhanced.

The efficiency of the digital medical image scrambling is achieved by the simplicity of the XOR operation. The true random scrambling key using chaos cryptography provides the security strength of this scrambling scheme.

Some critical features of this image scrambling algorithm are summarized in the following:

1. A true random encryption key is composed of the order of row-round scrambling and column-round scrambling, associated seed rows in each row-round scrambling and associated seed columns in each column-round scrambling.
2. The number of total rounds and the number of seed rows/column rows in each round are randomly chosen. For the number of total rounds, our experiments show that 15 rounds can normally achieve a reasonable flat histogram. More rounds can increase key space significantly. Users should strike a balance between the need for cryptographic strength and the real-time constraint.
3. In each row round/column round, the XOR operation is executed to all rows/columns of the images except the seed rows/seed columns. It is suggested that a column-round scrambling be introduced before the number of a consecutive row-round scrambling reaches the maximum rows of the original image and vice versa. As any two different grey values tend to have two different binary expressions, it is always possible to find a line along which 0 and 1 are randomly distributed. A random row and column scrambling can spread this randomness over the whole image.
4. This image scrambling process neither increases the size of the cipher image nor loses any information. The proposed image scrambling scheme operates on binary bit level which is exactly the same as many other existing encryption algorithms such as the DES. It does not incur extra cost in preparing the input data.

As the rows/columns for each scrambling are picked up randomly from the images, the binary value 1, 0 distributions of the strips (composed of seed rows and seed columns) are not correlated. The grey level values in the scrambled image will be uniformly distributed if the scrambling is repeated for enough number of times.

3. Performance evaluation

Take a size 568×568 with eight-bit grey level value magnetic resonance images as an example, the image is shown as in Fig. 5a, and the histogram of this image is as shown in Fig. 5b.

3.1. Image scrambling

Before scrambling, each pixel is first sliced into eight-bit binary values, i.e. converted into its corresponding binary image. Therefore, XOR could be directly operated to any two rows/columns. Then, a true random number sequence is generated from the

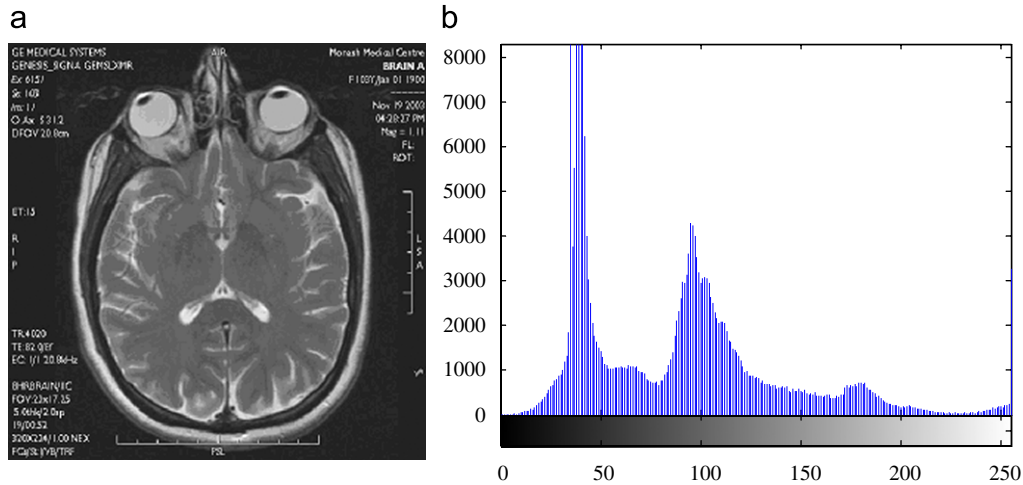


Fig. 5. MRI image and its histogram: (a) MRI image (http://www.southernhealth.org.au/imaging/35_mri.jpg) and (b) histogram.

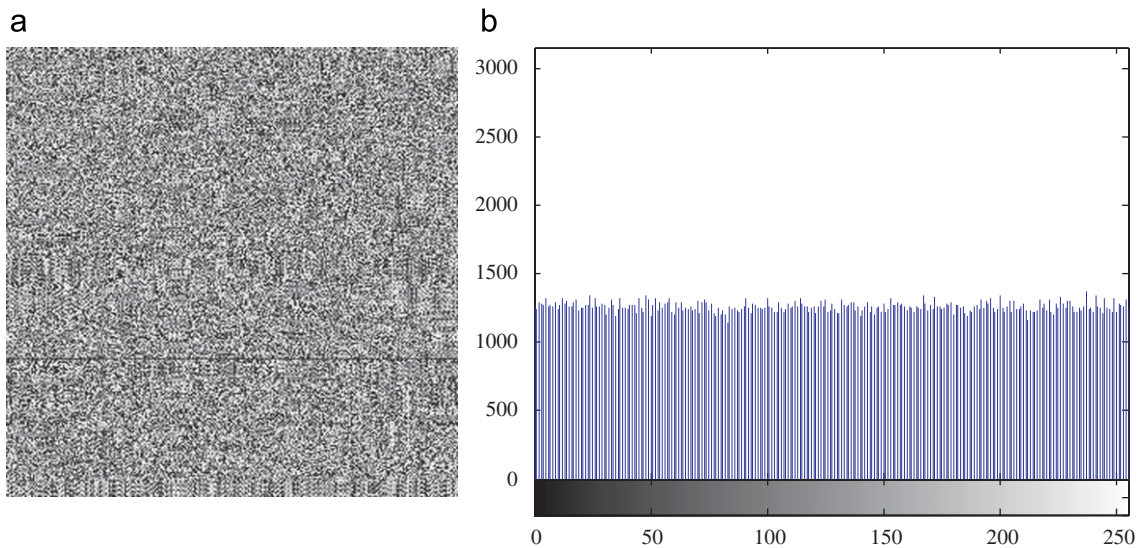


Fig. 6. After 10 rounds XOR operation: (a) scrambled image and (b) histogram.

multi-scroll chaotic attractors as demonstrated in Section 2.2. When $a = 1$, $b = 0.125$, $p = 6$, $q = 4$ with initial conditions (4.5683, 2.9367), the first 27 bits random number sequences from state variables x and y are:

```
[011100010 010010101 100110110],
[010111010 110001011 000111010].
```

After that, based on the TRN sequences, rows 226, 149, 310 are picked up and constitute a 3×568 row seed block which is used to XOR with other rows of the image (except row 226, 149 and 310). And the columns 186, 395, 58 are picked up and constitute a 568×3 column seed block, which is used to XOR with the other columns of the image (except column 186, 395 and 58). Note that while XOR-ing, the corresponding rows 226, 149, 310 and columns 186, 395, 58 are kept unchanged. Till now, the first round XOR operation, consisting of one row-round and one-column round, has been completed.

The procedure is repeated for 10 rounds. For each round XOR operation, different three rows and three columns are picked up based on the two random number sequences extracted from state variables x and y . The scrambled image and the histogram are as

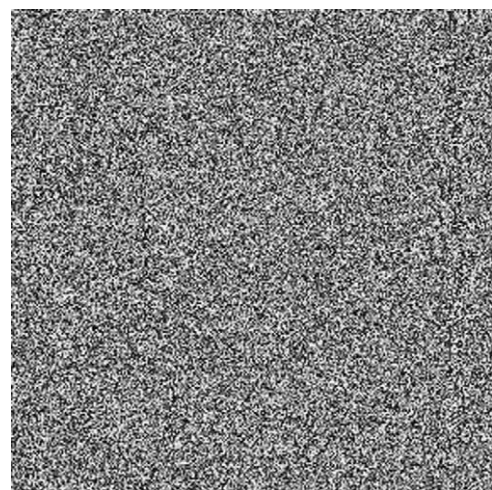


Fig. 7. Scrambled image after 30 rounds XOR operation.

shown in Fig. 6a and b. After 30 rounds of XOR operation, the scrambled image is shown in Fig. 7, the histogram of which is also flat like in Fig. 6b.

One can conclude from Figs. 6 and 7:

1. From Fig. 6b, after 10 rounds XOR operation, the pixel value is almost uniformly distributed, therefore, the histogram has been made flat.
2. Comparing Fig. 6a with that of Fig. 7, with the increase of the scrambling rounds, the scrambled image becomes more randomly visual.

Note that this ISA mechanism also applies to other images because of the pixel-based scrambling. Any grey level image can be converted into a binary image. As a result, with enough round of XOR operation, the neighbouring pixel can be fully scrambled.

3.2. Encryption efficiency

It has been concluded that for encryption efficiency, the 256-bit AES encryption is recommended to secure digital medical data (Snyder, 2003). However, it can only deal with very limited digital medical data. The encryption of 16-bit grey level MRI and other higher imaging modalities, such as CT and mammography, the above-mentioned encryption algorithm is computational exhaustive. In our experiment, the efficiency of the proposed ISA algorithm has been compared with the AES in a 2.0G 486 computer. The cryptographic key generation using our proposed chaotic theory takes a very small amount of time and is usually at several milliseconds scale. The encryption of the above MRI image using the ISA algorithm is around 0.002 s (30 rounds), which is more than 100 times faster than that of the AES.

3.3. Key space and statistical analysis

Preliminary analysis indicates that each row/column number could be represented with 9-bit binary for the size 568×568 images. Therefore, the first 27 bits TRN sequence from state variable x is the key for the first round row scrambling; the first 27 bits from state variable y is the key for the first round column scrambling. In this example, with 10 rounds of scrambling, each time three rows and three columns are picked up. And the key space is as large as $(27+27) \times 10 = 540$ bits. To choose the key for each round XOR operation with three rows and three columns, one has the following number of possible combinations:

$$2C_3^{568} C_3^{568}, \tag{5}$$

where parameter 2 accounts for the order of performing row-round scrambling and column scrambling. For 10 rounds of image scrambling, it will generate following number of possible combinations:

$$(2C_3^{568} C_3^{568})^{10} \approx 2^{510}. \tag{6}$$

The final key space for exhaustive search is given by

$$\min\{(2C_3^{568} C_3^{568})^{10}, 2^{540}\} = 2^{510}. \tag{7}$$

For a 486 computer with 100M CPU, assuming a computer program can try a million keys per second, it will take more than $(10)^{140}$ years to find the correct key. The above analysis assumes that each round uses three seed rows and three seed columns and 10 rounds and this information is known to the attackers. The key space can be easily expanded further by more complicated combination of row-round scrambling and column-round scrambling. Actually seed rows in each row-round scrambling can be from 1 row to 567 rows and it is the same for the seed columns in each column-round scrambling. This will expand the key space significantly. The space of true random number can also be expanded by adopting more chaotic scrolls. For the traditional AES

encryption, breaking an 80-bit or higher key is still extremely difficult, while the key space in this paper can be much longer than 80-bit.

The randomness in the choice of rows/columns can contribute to the entropy. One can see that the histogram in Fig. 6b shows preferable statistic characteristics against spectrum cryptanalysis, which means the resulting encrypted image can create a random looking image with a uniform histogram. Therefore the scrambled images can be well hidden.

The round number of this proposed encryption scheme is based on the security level and the length of the key in each round considering the balance between security and efficiency. Usually, 30 rounds are enough for a key length of 80 bits.

In principle, the proposed ISA scrambling algorithm is a linear scheme. Assuming that a 586×586 eight-bit grey level image is to

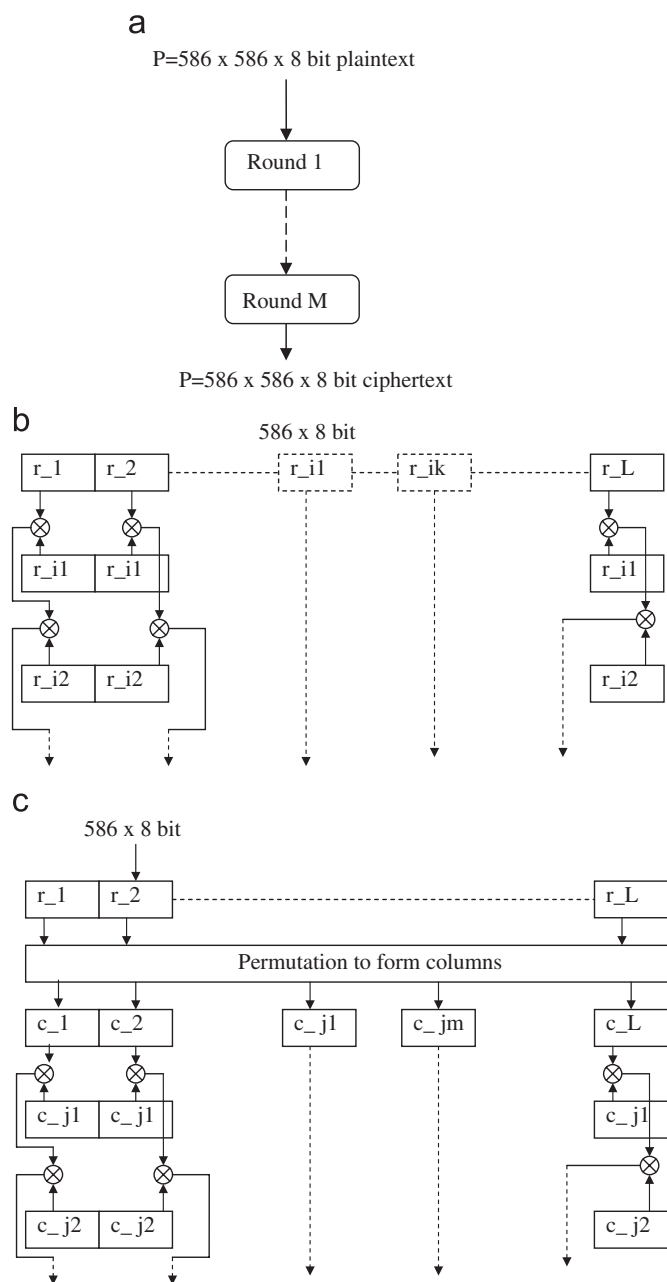


Fig. 8. (a) Overall structure of ISA scheme, (b) RRS operation with (r_{i1}, \dots, r_{ik}) being seed rows. Dotted components (r_{i1}, \dots, r_{ik}) in the input are not XORed and (c) CRS operation with (c_{j1}, \dots, c_{jm}) being seed columns. Dotted components (c_{j1}, \dots, c_{jm}) in the input are not XORed.

be encrypted, then we have the input plaintext by appending the image data row by row with $L = 586$. The ISA scrambling scheme is illustrated in Fig. 8 where each complete round, i.e., ORS, of scrambling consists of mixed RRS and CRS operations.

For a row-round operation, the ciphertext is given by $C_i = Fr(P_i, i_1, \dots, i_k)$, where P_i is the plaintext text input to the i th round of row operation Fr . Similarly for a column-round operation, the ciphertext is given by $C_i = Fc(P_i, j_1, \dots, j_m)$. The overall operation is given by a random concatenation of RRSs and CRSs as follows:

$$Fr(P_1, i_1, \dots, i_k) \circ Fc(P_2, j_1, \dots, j_m) \dots \dots \dots \rightarrow \text{End of } M \text{ rounds.} \quad (8)$$

Note the difference between the ISA scheme and conventional cryptographic schemes such as the DES. In the DES scheme, the scrambling structure is fixed and public known and the security strength is achieved by the introduction of the nonlinear S-boxes and the secret value of the external key. While in our ISA scheme, $i_1, \dots, i_k, j_1, \dots, j_m$ and M form an integral part of a random cryptographic key and are structural parameters. Without knowledge of this key, it is impossible to find explicit expression of the output produced by the $M-1$ rounds of scrambling, which is needed for linear cryptanalysis attack and differential cryptanalysis attack (Biham and Shamir, 1991; Matsui, 1994). Brute-force search of these parameters is infeasible due to the large key space.

4. Conclusions

In this paper, a digital medical images protection scheme has been proposed. Simple XOR operation is used to scramble the original images which could achieve a high efficiency. The scrambling key is a true random number sequence derived from the multi-scroll chaotic attractors. The cryptographic security strength of the image scramble scheme is provided by the true random number sequence and large key space. The generation of the cryptographic key using the chaotic theory is at the scale of several milliseconds in our example. The same scrambling key can be reused for multiple sessions which is the same as in many other asymmetric block cipher encryption schemes. Hence the overhead of a key generation and distribution is mitigated.

Experiment and spectrum analysis have validated the effectiveness of the proposed scheme. Our proposed ISA image scrambling scheme is more than 100 times faster than that of the popular AES, which renders it a suitable candidate for real-time encryption of large digital medical images. For secure distribution of the scrambling key, a bio-cryptosystem can be deployed (Han et al., 2005; Wang et al., 2007).

Acknowledgement

The work is financially supported by the Australia Research Council (ARC) Projects with project IDs LP0455324 and DP0985838.

References

Ashtiyani M, Birgani PM, Hosseini HM. Chaos-based medical image encryption using symmetric cryptography, information and communication technologies: from theory to applications, 2008. In: Proceedings of the 3rd international conference on information and communication technologies, 2008. p. 1–5.

- Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology* 1991;4(1):2–72.
- Boring CC, Squires TS, Tong T. Cancer Statistics, CA, A Cancer Journal for Clinicians 1992;42:19–38.
- Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals* 2004;21(3):749–61.
- Chiarelli A. Invisible cryptography—a medical application. Retrieved at <http://www.physics.uwo.ca/teamcana/2004/chiarelli_report.pdf>, 2004.
- Coatrieux G, Quantin C, Montagner J, et al. Watermarking medical images with anonymous patient identification to verify authenticity. *Studies in Health Technology and Informatics* 2008;136:667–72.
- Dawson E, Nielsen L. Automated cryptanalysis of XOR plaintext strings. *Cryptologia*, April 1996.
- Dickson KW Chiu, Patrick CK Hung, Vivying SY Cheng, Eleanna K. Protecting the exchange of medical images in healthcare process integration with web services. In: Proceedings of the 40th Annual Hawaii international conference on system sciences, 2007.
- Formazin M, Netto Jr DBS, Cavenaghi MN, Marana AN. Protecting medical images with biometric information. *Advances in Computer and Information Sciences and Engineering* 2008:284–9. http://www.southernhealth.org.au/imaging/35_mri.jpg.
- 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;39:1636–7.
- Han F, Hu J, Yu X, Feng Y, Zhou J. A novel hybrid crypto-biometric authentication scheme for ATM based banking applications. In: Proceedings of the international conference on biometrics (ICB). Lecture notes in computer science, vol. 3832, 2005. p. 675–81.
- 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):1004–8.
- Hu J, Bertok P, Tari Z. Taxonomy and framework for integrating dependability and security, [Chapter 6]. Morgan Kaufman, Imprint of Elsevier; 2008. p. 149–70 [Information Assurance: Survivability and Security in Networked Systems].
- Kodama N, Shimada T, Fukumoto I. Image-based diagnosis of Alzheimer-type dementia: measurements of hippocampal and ventricular areas in MR images. *Magnetic Resonance in Medical Science* 2002;1(1):14–20.
- Lou SL, Sickles EA, Huang HK. Full-filed direct digital mammograms: technical components, study protocols, and preliminary results. *IEEE Transactions on Information Technology in Biomedicine* 1997;1:270–8.
- Matsui M. Linear cryptanalysis method for DES cipher. Workshop on the theory and application of cryptographic techniques on advances in cryptology. Lofthos, Norway, 1994. p. 386–97.
- Montagnat J, Bellet F, Benoit-Cattin H. Medical images simulation, storage, and processing on the European DataGrid testbed. *Journal of Grid Computing* 2004;2(4).
- National Digital Medical Archive, Inc. Provides tools to enable sharing of digital medical images. <<ftp://ftp.software.ibm.com/software/solutions/pdfs/ODB-0148-02.pdf>>; Retrieved in 2008.
- Norcen R, Podesser M, Pommer A, Schmidt HP, Uhl A. Confidential storage and transmission of medical image data. *Computers in Biology and Medicine* 2003;33:277–92.
- Pareschi F, Setti G, Rovatti R. A fast chaos-based true random number generator for cryptographic applications. In: Proceedings of 26th IEEE European solid-state circuit conference, Montreux, Switzerland, September 11–14, 2006. p. 130–3.
- Rahman MM, Wang T, Desai BC. Medical image retrieval and registration: towards computer assisted diagnostic approach. In: Proceedings of the IDEAS workshop on medical information systems, 2004.
- Snyder AM. Performance measurement and workflow impact of securing medical data using HIPAA compliant in a .NET environment. Master degree thesis, University of Virginia, 2003.
- Wang JZ. Security filtering of medical images using OCR. Digital libraries: advanced methods and technologies, digital collections. In: Proceedings of the 3rd all-Russian scientific conference, Petrozavodsk, Russia, September 2001. p. 118–22.
- Wang Y, Hu J, Philip D. A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing. Special issue on Biometrics: Progress and Directions. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 2007;29(4):573–85.
- 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):1395–404.
- Yang M, Bourbakis N, Li S. Data-image-video encryption. *IEEE Potentials* 2004;28–34.
- Zhou XQ, Huang HK, Lou SL. Authenticity and integrity of digital mammography images. *IEEE Transactions on Medical Imaging* 2001;20(8):784–91.
- Ziv Y, Leo J. Long bone panoramas from fluoroscopic X-ray images. *IEEE Transactions on Medical Imaging* 2004;23(1):26–35.