JOURNAL OF APPLIED SCIENCES RESEARCH

JOURNAL home page: http://www.aensiweb.com/JASR 2015 March; 11(4): pages 10-29.

Published Online: 15 January 2015. **Research Article**

Statistical Analysis of One Time Pad Encryption Using Variable Chaotic Key for Medical Data Transmission & Storage

[1]Mohammadreza Naeemabadi, [1,2]Alireza Mehri Dehnavi, [1,2]Hossein Rabbanni, [3]Kambiz Bahaadinbeigy, [4]Hassan Khajehpour

[1]Department of Biomedical Engineering, School of Advanced Medical Technologies, Isfahan University of Medical Sciences, Isfahan, Iran.
[2]Medical Image & Signal Processing Research Center, Isfahan University of Medical Sciences, Isfahan, Iran.
[3]Medical Informatics Research Center, Kerman University of Medical Sciences, Kerman, Iran.
[4]Department of Medical Physics & Biomedical Engineering, School of Medicine, Tehran University of Medical Sciences, Tehran, Iran.

Received: 25 November 2014; **Revised:** 26 December 2014; **Accepted:** 1 January 2015

ABSTRACT

According to increasing application of wireless communication techniques in medical data transmission, data privacy and security are crucial. Currently there are several algorithms that function as data encryption methods. These algorithms often use a pre-determined constant key of minimum 128 bits long. Quasiperiodic characteristics of medical data and same encryption keys lead to periodic behavior of the encrypted data, which undermines the security. In this paper the key for each block encryption changes by applying a chaotic series, and it is not easily possible to derive one key in accordance to the previous one. In order to evaluate quality, efficiency and security of this method, a comparison was made between this method and the most powerful encryption method of Rijndael by means of seven factors. The largest share of employed data for evaluation purpose is cardiac clinical records. Lower noise sensitivity (30 times lower), faster (almost 27 times more), and higher pattern hiding ability are advantages of the proposed method over traditional Rijndael.

Keywords: Medical Record Encryption, Chaotic Series, Medical Signal Encryption, One Time Pad, Encryption Quality, Efficiency and Security Analysis of medical data, medical data privacy.

INTRODUCTION

Development in telecommunications technology and especially wireless communications, raise the need for data encryption and hiding. Furthermore data privacy can be obtained only through encryption techniques. Innovative techniques' presence in medical science and engineering implementation in medicine made significant improvement in offered services in recent decades. In addition, in the last decade telecommunications technology were employed in medicine aiming to transmit medical data, create telemedicine and electronic health care. Data transmission strongly needs to be provided with communication and data security and privacy. Network security problems are generally divided into four closely related categories: (1) Secrecy, (2) Authentication, (3) Non-Repudiation and (4) Integrity control. Medical records of a patient may contain critical information that should not be accessible to non-authorized persons. Not only does keeping medical records of the patient inaccessible secures the patient privacy but also protect patient's data from being invaded and threatened. Patient's medical data invasion is done either from inside or outside the medical system. Invasion form outside the medical system is carried out by listening and or modifying the medical records through computer network attacks such as eavesdropping, packet injection, and man-in-the-middle attacks. Clinicians, patients or individuals at the health care service could be inside intruders. Motivations for invasion could be medical malpractice cover up and healthcare insurance fraud [1-3]. The most common procedure to preserve security and privacy of medical records is encryption. Although there has not been a proposed encryption method specifically for medical records, there are several methods that are implemented for encryption purpose regardless of the content. Blowfish, DES, IDEA, RC5, RC6, Triple DES, Rijndael, Serpent, and Twofish are the most common encryption methods with symmetrical key among which twofish, Rijndael, Serpent are the most successful ones. All these methods usually employ a 128 to 256 bits key [4-9].

The aforementioned encryption methods' security is guaranteed by complex processes while encrypting. Moreover, according to the block encryption (block cipher design), error sensitivity significantly rises in the stream data transmission. A new encryption method combined of one time pad encryption algorithm and chaotic systems is introduced in this paper. This method is simple and has unique efficiency in medical records encryption.

Corresponding Author: Mohammadreza Naeemabadi, Department of Biomedical Engineering, School of Advanced Medical Technologies, Isfahan University of Medical Sciences, Isfahan, Iran.

The section 2 contains the proposed method and Rijndael method descriptions. The employed data in this study are introduced in section 3. The comparison and evaluation of the proposed method is carried out by 7 factors in section 4 and the conclusion regarding the implemented method could be reached in section 5.

Implemented method:

The proposed encryption method employ one time pad encryption method beside chaotic system generates the encryption key.

The key produced by chaotic system does not have the periodic characteristic, it does not converge or diverge, and chaotic system creates a key set. This key set is chaotic as well therefore it is not easy to get one key according to its previous one. The next step is to perform one time pad encryption method employing these keys. Further in this section Rijndael and one time pad encryption methods are described.

2-1 Advanced Encryption Standard:

Nowadays symmetric encryption gained higher popularity in comparison with conventional encryption methods (substitution and transposition) mainly due to its high complexity. These methods are called symmetric because the decryption and encryption are performed using the same key.

In cryptography terminology, the data to be encrypted, the employed encryption key and the encrypted data are regarded as Plaintext, cipher key and Ciphertext respectively. The intruder who solely keeps data under surveillance and who modifies the encrypted message are appointed as passive and active intruders respectively in cryptography.

As a consequence of breaking DES encryption 1997, the NITS decided to introduce a new and powerful encryption system with Advanced Encryption System code name [10].

In 1998, Serpent ،Rijndael ،Twofish ،RC6 and MARS algorithms took a part in AES election contest. Rijndael algorithm won this competition in terms of security, efficiency, simplicity and memory requirements priorities.

Rijndael encryption algorithm employs 128, 192 and 256-bits cipher keys and 128-bits Plaintext block size. This algorithm consists of several rounds; and each round, except first round (or round zero), has four steps.

In contrast with DES, which performs on bits, Rijndael goes on bytes. Therefore it is easier to implement Rijndael rather than DES both on software and hardware perspectives.

The initial phase takes place before any rounds get started. The initial round is also called the key expansion step, since certain numbers of round keys are generated from the main key. Key generation procedure illustrated in Figure.1.

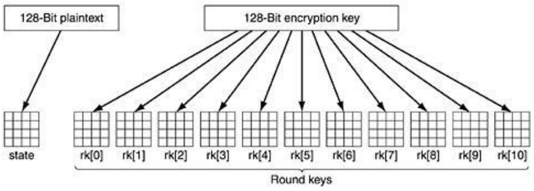


Fig. 1: Initial phase, the key expansion.

Each round key belongs to a specific round and it is only utilized in its corresponding round. In round zero the 128-bit block is placed in a 4×4 two dimensions array, which is called state. This array is updated in each step of round. Having state array built, in round zero this array is XORed byte by byte to the zero round's key; this procedure is repeated in every round with corresponding round key.

In the first step, substitution step, byte by byte substitution of components of state array with new values take place through s-box. This process done by monoalphabetic substitution.

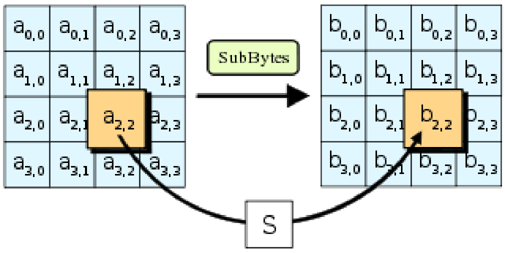


Fig. 2: SubByte Step.

The second step, shift rows step, in each row bytes are shifted to the left according to the number of the corresponding row's number. Subsequently, first row or row number zero stays untouched; row number one is shifted one byte to the left, row number two is shifted two bytes to the left and row number three is shifted three bytes to the left. Figure 3 presents this row shifting process.

In third step, mix columns, columns are mixed individually. In this process the state array is multiplied by a Finite Glaois Field modulo. To simplify this step look-up tables are employed. Each new column is obtained by two times search in the look-up table and three XORs.

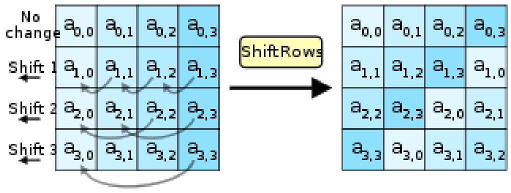

No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig. 3: Shift rows step.

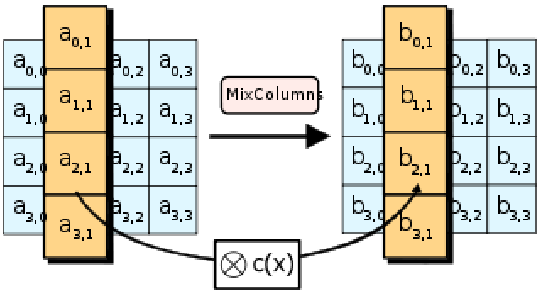

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig. 4: The mix columns step.

Finally in the fourth step, the round key is XORed byte by byte to the state array. Figure 5 shows the process in the fourth step. Rijndael decryption and encryption are different in permutations' and substitutions' order [11, 12].

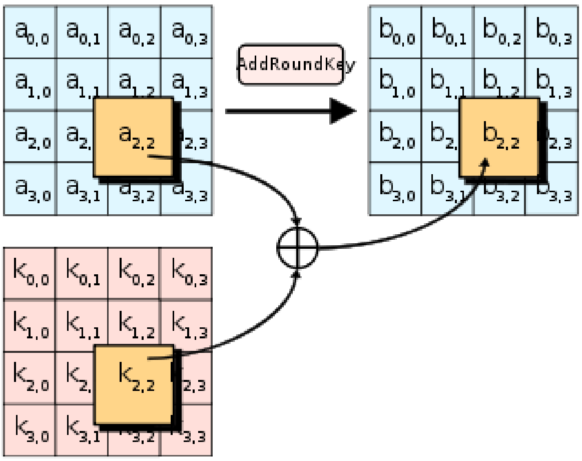

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Fig. 5: Add Round Key Step.

2-2 OPT Encryption method:

In 1882, for the first time Frank Miller introduced OTP encryption in telegraphy. In 1917, Gilbert Vernam invented an electrical implementation of this encryption method and patented it as teleprinter in 1919 [13]. In this method each character of the message is electrically combined with a punched tape key; this key was repeated in a loop.

Later on Joseph Mauborgne found out if the key is perfectly accidental and random with the same length of message it is impossible to decrypt a message without having the key.

Logical gates and circuits being available, the onetime pad encryption method could be easily implemented by a two-input XOR gate. Having the string bit message and the key as XOR gate inputs, the output is the Cipher message.

Having the string key, it is easy to decrypt the message by an XOR gate; while the key and Cipher message are the inputs and the original message is the output.

Given P and K are the original plaintext and the cipher key respectively, their XOR will be C which is the Ciphertext. D is the decrypted message and also C xored K output. The OTP decryption and encryption methods are defined as (1):

$$C = P \oplus K = \begin{cases} 1 & if\, P \neq K \\ 0 & if\, P = K \end{cases} \qquad (1)$$

$$D = C \oplus K = \begin{cases} 1 & if\, C \neq K \\ 0 & if\, C = K \end{cases}$$

The continuous equality of the original and decrypted Cipher data is illustrated in Table1.

Figure 6 depict a simple scheme of OTP encryption and decryption implementation by XOR gate.

Table 1: OTP accuracy evaluation; P: original message; K: encryption key; C: Cipher message; D: decrypted message.

P	K	C	D
0	0	0	0
	1	1	0
1		0	1
	0	1	1

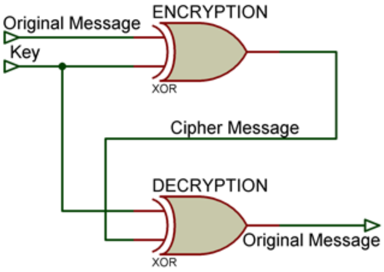


Fig. 6: Encryption and decryption method with two XOR gate.

It can be easily inferred from Figure 6 that the OTP is uniquely simple in comparison with other encryption methods. Apart from simplicity, if the encryption key follows Shannon security it is impossible to decrypt without having the key [14, 15].

So, not only the key must be random and unpredictable but also the key and the plaintext should be of the same length. Consequently application of cryptographically secure pseudorandom number generator (CSPRNG) gained high level of importance as a key and there were many attempts to obtain a totally random unlimited-length key[16, 17].

In this paper an unpredictable infinite-length key is generated by chaotic system employed; this key is only producible by having the chaotic system's input.

The encryption modes of ECB and CBC are implemented which are further explained in the following sections.

2.2.1 ECB mode of OTP Encryption:

ECB encryption mode is the most straightforward encryption mode. In this mode each byte of plaintext is encrypted by the key individually. If the Plaintext consists of n bytes, it is divided to n parts: P_1, P_2…, P_n. The Ciphertext is obtained by encryption of each part separately in form of C_1, C_2… C_n. Decryption is also implemented on each part with the key separately. The encryption and decryption methods are defined in (2) and represented in Figure7. E_k and D_k represent encryption and decryption algorithms respectively, as it was stated earlier in this paper encryption and decryption algorithms are the same in OTP. It should be mentioned that ECB encryption mode in OTP algorithm categorized as prefect stream cipher encryption algorithm.

$$C_i = E_K(P_i) = K \oplus P_i \quad i = 1,.., n \qquad (2)$$

$$P_i = D_K(P_i) = K \oplus C_i \quad i = 1,..., n$$

Independently encrypting blocks, in addition to the simplicity avoids the error propagation from one bit or byte to other parts. So, this method is expected to have low noise sensitivity.

The most distinguished weakness with this method is that it does not hide the data pattern which can be easily seen in the images. This failure is illustrated in Figures 21-23 [18-20].

2.2.2 CBC mode of OTP encryption method:

The CBC mode is similar to EBC mode except that before encryption by the key, the plaintext byte is XORed with the previous encrypted byte. Encryption and decryption in this mode are stated in (3):

$$C_i = E_K(P_i \oplus C_{i-1}) = K \oplus (P_i \oplus C_{i-1}) \quad i = 1,.., l \qquad (3)$$

$$P_i = D_K(P_i) \oplus C_{i-1} = (K \oplus C_i) \oplus C_{i-1} \quad i = 1,..., l$$

It can be seen from (3) that one byte from previous encryption is employed in the current encryption; therefore for the first data to be encrypted an initial value (IV) of zero is assigned to C_0. Figure 8 and 9 illustrate the encryption and decryption in CBC method[21]. CBC mode can assume as rudimentary form of block cipher encryption algorithm.

The length of the block, which is encrypted in accordance with other blocks, is shown by *l* in (3). The larger block length improve pattern hiding of plaintext especially for images with obvious pattern. The large-length block deals with the weakness of ECB in hiding the image.

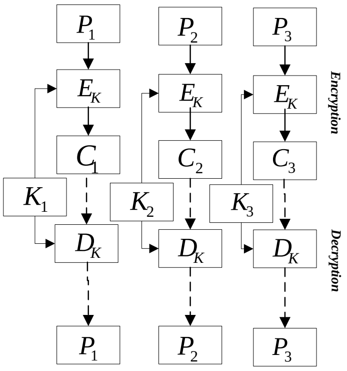


Fig. 7: ECB mode of OTP encryption and decryption method.

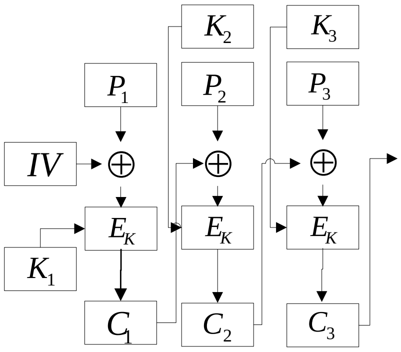


Fig. 8: CBC mode encryption.

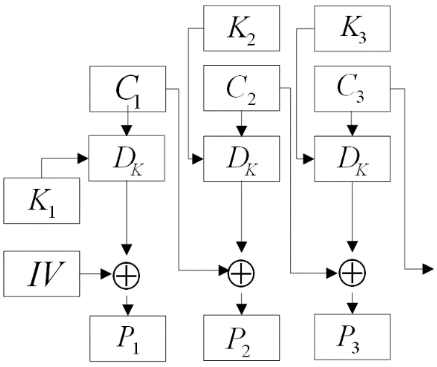


Fig. 9: CBC mode Decryption.

Considering that each byte is influenced by previous bytes, the noise in one byte is scattered to other next ones.

EBC can be regarded as CBC with block length of 1.

2.2.3 OTP method encryption key:

As it was mentioned earlier, in OTP encryption method infinite length unpredictable random key makes decryption to be impossible without key. The key with these specific characteristics can be achieved by random number generators. Since having the key is essential for decryption the key should be transmitted along with the encrypted data. Transmission of the key alongside the message threatens the security as well as doubles the data volume.

As a solution to the above mentioned problem, a key with aforementioned characteristics which could also be produced at decryption section with having little initial information is proposed. Incorrect information makes generating the key impossible. Chaotic systems are well capable of producing the key with the above mentioned features[22, 23].

In this paper a chaotic system is employed to generate the keys. The Mackey Glass series is one kind of chaotic series. It is worth mentioning that chaotic systems possess following features:

- Non-linear
- High initial condition sensitivity
- Non repeatable trajectory over time
- Entering the chaotic state by means of numerous branches

- Fractal dimension behavior

The Mackey series is defined in (4):

$$\frac{dx}{dt}=\frac{(ax(t-\tau))}{(1+x^{n}(t-\tau))}-bx(t) \qquad (4)$$

In (4) a, b and n are constant values, τ is the delay. The equation chaotic behavior starts at *τ≥17*. The equation has initial conditions on which it strongly depends [24-26].

In this paper constant values of 0.2, 0.1, 10 and 20 are assigned to a, b, n, and *τ* respectively. The only variable parameter is the initial condition, so the equation (4) is simplified to (5):

$$\frac{dx}{dt}=\frac{[0.2x(t-20)]}{[1+x^{10}(t-20)]}-0.1x(t) \qquad (5)$$

Two time series with a slightly different initial condition, 1e-7 difference, and their difference is shown in Figure 10. As it can be seen from Figure 10, a small difference in initial condition leads to a considerable difference in final results.

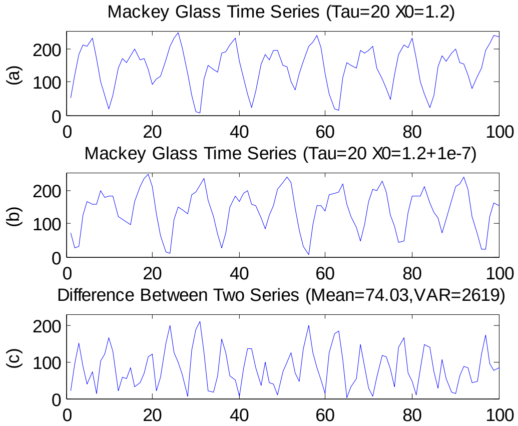


Fig. 10: (a): Mackey Glass time series with initial condition of x0=1.2; (b): Mackey Glass time series with initial condition of x0=1.2+1e-7; (c): Difference between (a) and (b).

Space state diagram or Poincare section of two series, with a unit point difference in initial conditions, is shown in Figure 11. It can be easily inferred that a slight change in initial condition results in a huge output difference.

2.3 Implementation of One time pad encryption employing chaotic key and Rijndael:

The intruder may have access to Ciphertext only, or part of Ciphertext and Plaintext. The intruder may be able to change any part of the Plaintext to Ciphertext and encryption algorithm should present robust security against these situations.

Kreckhoff principle states that encryption procedure should be clear and public, only the key needs to be hidden and concealed. Consequently, the intruder may be able to decrypt some parts of the data or even find out the key. Figure 12 illustrates the employed methods in this paper.

In Rijndael, cases that are encrypted with a constant key that is periodic, with a period larger than the block's length, in some intervals the encrypted data may be periodic. This problem escalates when data is located in a frame with certain header and trailer. The intruder may as well insert invalid encrypted data without any information about the original signal.

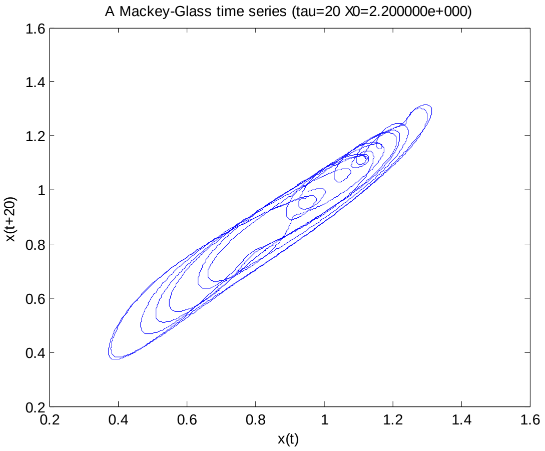


Fig. 11a: Mackey Glass time series with initial condition of x_0=2.2.

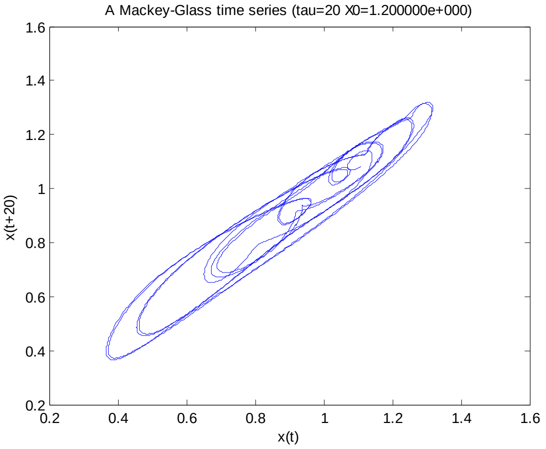


Fig. 11b: Mackey Glass time series with initial condition of x_0=1.2.

In the proposed method even if the output signal is constant the encrypted signals is not periodic. Repeatedly changing key makes it possible to get various outputs for constant input.

Figure 13 shows that constant input result in a constant output. While in Rijndael given the block is 128 bits, the output will be periodic in 8-bit blocks.

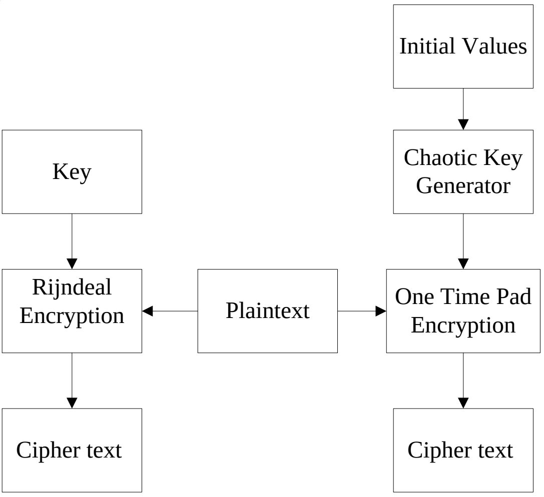


Fig. 12: Encryption method block diagram.

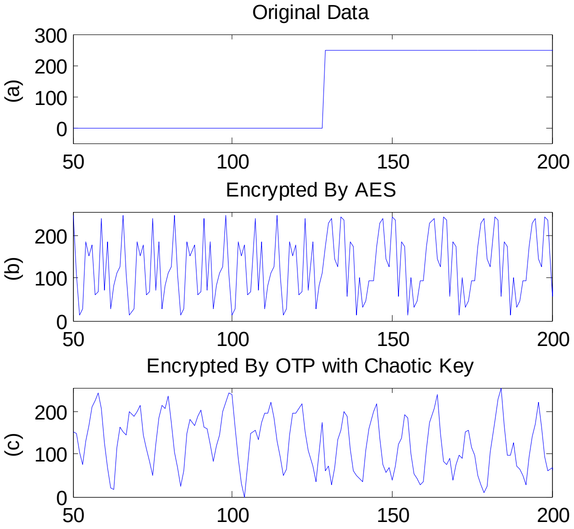


Fig. 13: (a) Original data; (b) Encrypted data by AES; (c) Encrypted data by OTP in ECB mode.

3. Data:

To evaluate the algorithm four groups of dataset are employed. The first dataset consists of 10 Electrocardiogram signals from MIT- BIH data set. The employed records are 103, 109, 212, 209, 123, 117, 116, 111, 231 and 230[27].

Second series of data comprise 4 photocardiogram signals. These signals are derived from pec52.dat, pec33.dat, pec22.dat andpec1.dat data sets in Biomedical Signal Analysis book [28].

Third group data covers 60 cardiac CT taken by Simens SOMATOM sensation 64 slices at Isfahan Milad hospital [29, 30]. Figure 14 illustrates the employed cardiac CT images.

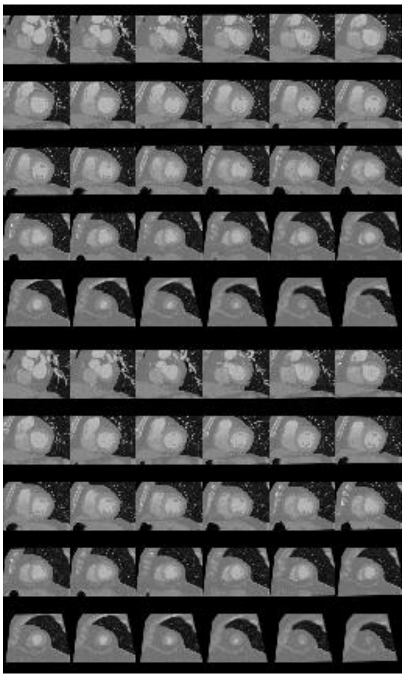


Fig. 14: 60 employed Cardiac CT for evaluation.

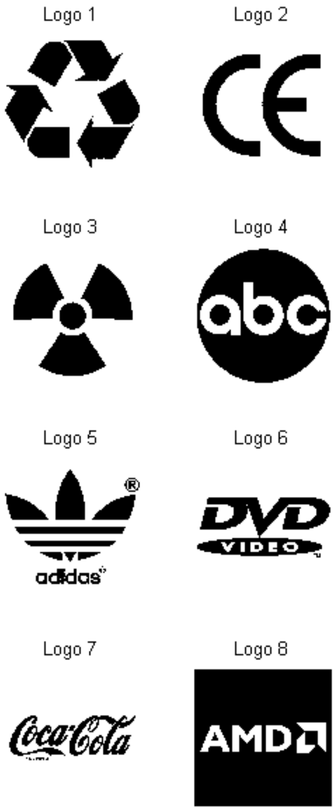


Fig. 15: Employed logo images for hiding capability evaluation.

Last dataset contains 8 logo images which are depicted in Figure 15, these images were used to evaluate the capability of the algorithm in hiding the original pattern after encryption and also spreading the histogram. All images have two colors (two color level of white and black); the four first ones encompass fewer details than the four last ones.

4. Evaluation and results:

Different algorithms were introduced for encryption methods evaluation up to now [31-34]. In this paper encryption quality, key sensitivity, noise sensitivity, speed and process time for each of AES and OTP encryption methods are evaluated. For OTP encryption method in CBC mode, block size of 2, 4, 16, 64, 128 and 256 are applied.

4-1 Encryption Quality or Maximum Deviation Factor:

Encryption quality has direct relation to the difference in Plaintext's and Ciphertext's histogram. Encryption quality calculated by (6)[21, 31].

$$EQ=\frac{\sum_{L=0}^{256}\left|Hist(P)-Hist(C)\right|}{256} \qquad (6)$$

In (6), Hist(P) and Hist(C) stands for Plaintext's and Ciphertext's histogram respectively. Table 2 shows encryption quality for above mentioned cardiac data. It can be clearly seen, the highest encryption quality rate belongs to OTP ECB mode, and Rijndael and OTP CBC 64 have similar encryption quality.

Table 2: Encryption quality of AES and OTP methods.

Mode	Block Size	Cardiac CT	ECG	PCG
OTP ECB		3.4521×10^5	45022	31172
OTP CBC	2	3.3030×10^5	40610	30110
OTP CBC	4	3.2460×10^5	39855	28847
OTP CBC	16	3.1111×10^5	39712	28017
OTP CBC	64	3.0573×10^5	39648	27679
OTP CBC	128	3.0481×10^5	39714	27716
OTP CBC	256	3.0416×10^5	39711	27509
Rijndael		3.3165×10^5	39732	27495

4-2 Correlation coefficient factor (CCF):

The second factor for evaluation of the encryption method is Correlation coefficient factor. This factor is the cross correlation of encrypted data and the original data. If this coefficient is closer to zero, the signals correlate less and vice versa. The encryption method quality is higher when the signals are less similar. The cross correlation is calculated by (7)[34, 35].

$$R_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)\times D(y)}}$$

$$\operatorname{cov}(x,y)= \qquad (7)$$

$$\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\times\left(y_i-E(y)\right)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

The results for cross correlation of original and encrypted data shown in Figure 16. According to this figure it can be seen that Rijndael and OTP CBC 256 gained smallest correlation.

4-3 Histogram:

Quality of the encryption method may also evaluate according to original data and encrypted data histogram[36]. The highest quality belongs to a method by which encrypted data histogram entirely spreads in all values comparing to original data histogram. Figure 17, 18 and 19 reveals a histogram change for ECG, EPG and Cardiac CT data respectively.

Based on the images, Rijndael and OTP CBC with block size of 64 or larger are able to spread the histogram over gray areas. Figure 19 shows that histogram did not perfectly spread by Rijndael.

Histogram of Logo1 from Figure 15 before and after encryption is displayed in Figure 20. As it was mentioned above these logos have two levels of white and black, therefore in comparison with other data sets it is more difficult for the histogram to be spread.

It can be inferred from Figure 20 that Rijdeal fails to spread the histogram it even functions weaker than OTP ECB. OTP CBC with block size of 64 bits and higher succeeded in histogram distribution.

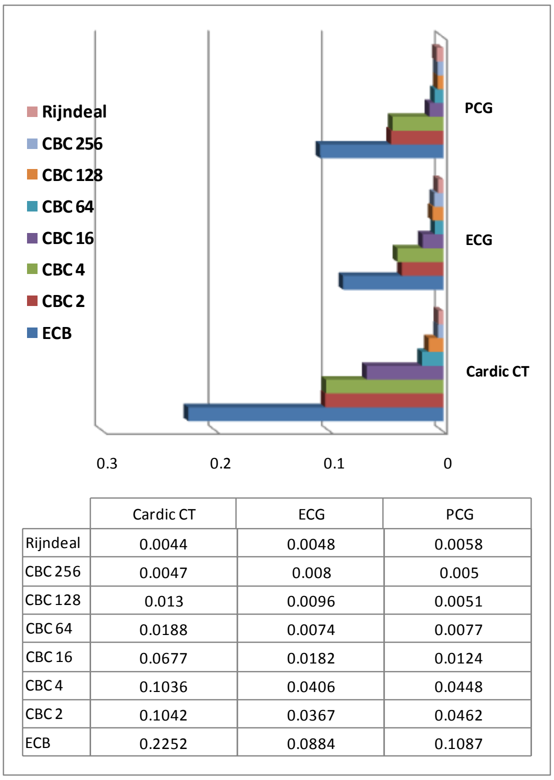
4-4 Pattern Hiding:

Covering up the pattern can be evaluated by image observation, similar to histogram; especially in images with extremely limited to a few gray levels it is more obvious.

Figure 21 illustrate encrypted image of one slice of the Cardiac CT image, histogram of which was illustrated in Figure 19.

Regarding the images encryption methods of OTP ECB, Rijndael and OTP BCB with block size up to 4 bytes failed to cover up the pattern.

Figures 22 and 23 shows logo1 and logo3 encrypted images with different methods. Considering large white and black areas and sharp edges in the original images it is easier that Cardiac CT images to distinguish the pattern.



	Cardic CT	ECG	PCG
Rijndeal	0.0044	0.0048	0.0058
CBC 256	0.0047	0.008	0.005
CBC 128	0.013	0.0096	0.0051
CBC 64	0.0188	0.0074	0.0077
CBC 16	0.0677	0.0182	0.0124
CBC 4	0.1036	0.0406	0.0448
CBC 2	0.1042	0.0367	0.0462
ECB	0.2252	0.0884	0.1087

Fig. 16: Cross correlation chart.

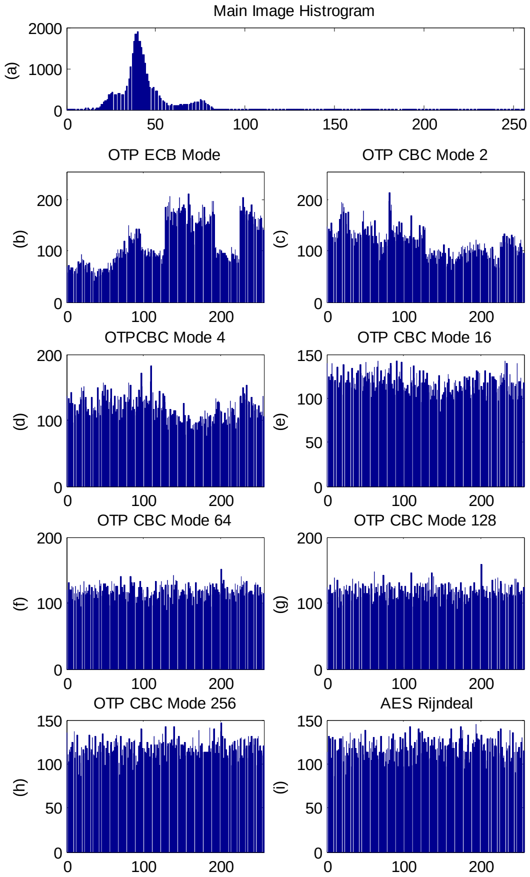


Fig. 17: An ECG signal histogram before and after encryption; (a) The original data histogram; (b) Histogram of the encrypted data by OTP ECB; (c- h) Histogram of encrypted data by OTP CBC with different block size; (i) Histogram of the encrypted data by Rijndael.

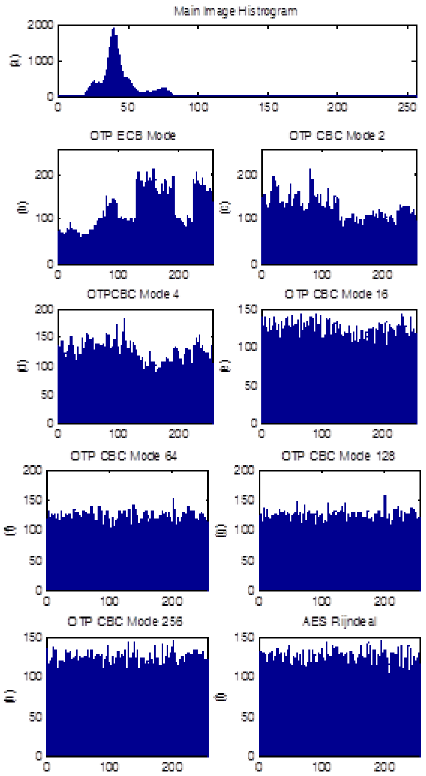


Fig. 18: APCG signal histogram before and after encryption; (a) The original data histogram; (b) Histogram of the encrypted data by OTP ECB; (c- h) Histogram of encrypted data by OTP CBC with different block size; (i) Histogram of the encrypted data by Rijndael.

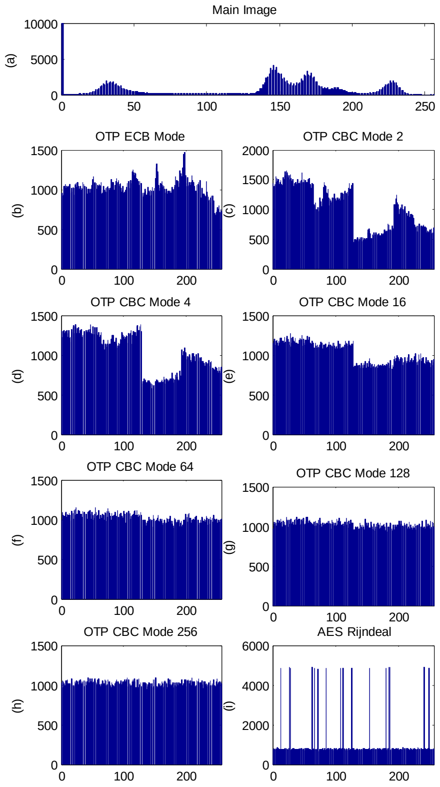


Fig. 19: A Cardiac CT image histogram before and after encryption; (a) The original data histogram; (b) Histogram of the encrypted data by OTP ECB; (c- h) Histogram of encrypted data by OTP CBC with different block size; (i) Histogram of the encrypted data by Rijndael.

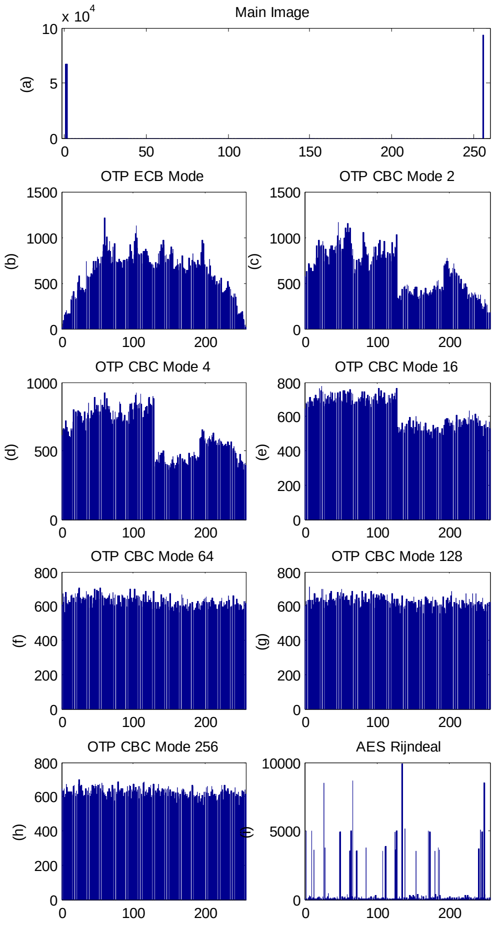


Fig. 20: A logo 1 image histogram before and after encryption; (a) The original data histogram; (b) Histogram of the encrypted data by OTP ECB; (c- h) Histogram of encrypted data by OTP CBC with different block size; (i) Histogram of the encrypted data by Rijndael.

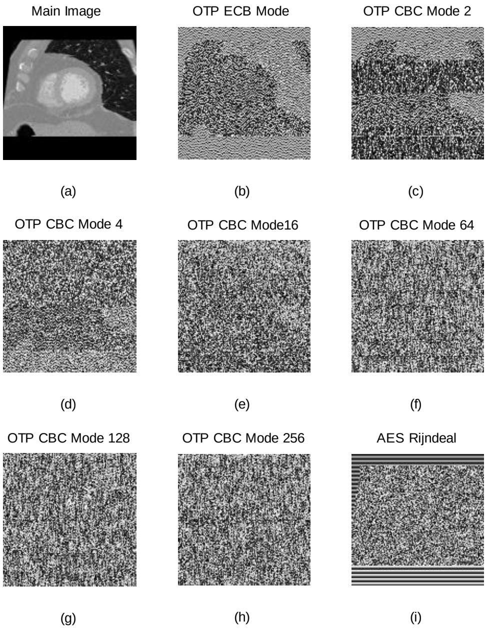


Fig. 21: A Cardiac CT slice image before and after encryption; (a) The original image; (b) The encrypted image by OTP ECB; (c- h) Encrypted image by OTP CBC with different block size; (i) Encrypted image by Rijndael.

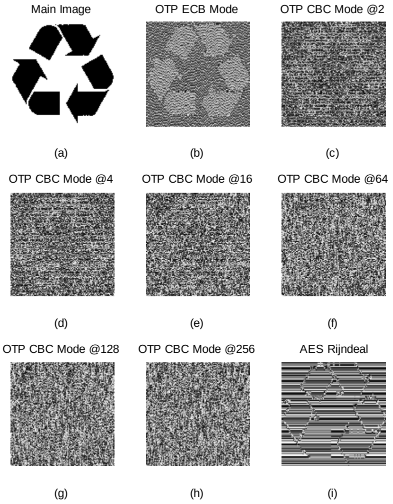


Fig. 22: Logo1 image before and after encryption; (a) The original image; (b) The encrypted image by OTP ECB; (c- h) Encrypted image by OTP CBC with different block size; (i) Encrypted image by Rijndael.

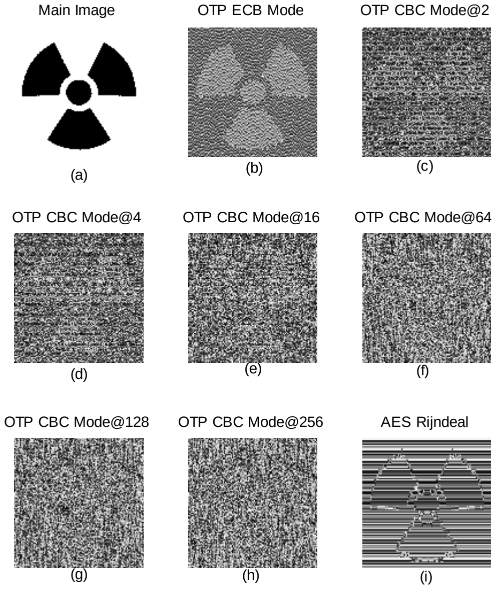


Fig. 23: Logo3 image before and after encryption; (a) The original image; (b) The encrypted image by OTP ECB; (c- h) Encrypted image by OTP CBC with different block size; (i) Encrypted image by Rijndael.

Figure 22 and 23, prove the point previously claimed about failure of Rijndael, ECB and CBC mode with narrow window size in last paragraph.

4-5 Process time and throughput:

Encryption speed and process time are important features of each encryption method. The process time for encryption depends on performed computations and tasks during encryption.

A powerful encryption method offers higher level of security with lower computation load. Encryption method with complex and heavy computations is not an appropriate method.

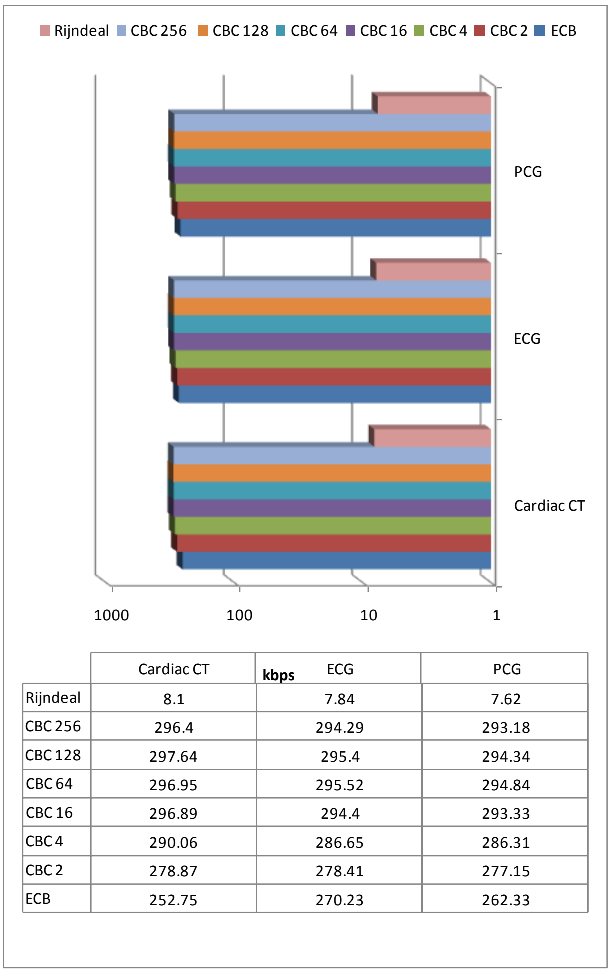
Average process time of different encryption method for encryption of each part of the ECG and PCG signals and each Cardiac CT image could be found in Table 3. The encryption is performed by a Intel Core 2 Quad Q6600 processor desktop with 4GB memory on Windows 7 64-bit operating system and Matlab2011a 64-bit software.

According to Table 3 the process time decrease as the block size increases in OTP method. Rijndael process time is 37 times higher than that of OTP.

Encryption speed or output rate is inversely related to the process time. The chart in Figure 24 presents the throughput of different encryption methods in kbps. This chart supports that OTP is significantly faster than Rijndael.

Table 3: Process time of AES and OTP encryption methods.

Mode	Block Size	Cardiac CT	ECG	PCG
OTP ECB		11.2358	0.8659	0.6099
OTP CBC	2	7.3440	0.8405	0.5773
OTP CBC	4	7.0607	39855	0.5588
OTP CBC	16	6.8981	0.7949	0.5455
OTP CBC	64	6.8968	0.7918	0.5427
OTP CBC	128	6.8809	0.7921	0.5436
OTP CBC	256	6.9095	0.7951	0.5458
Rijndael		252.7497	29.8439	20.9993



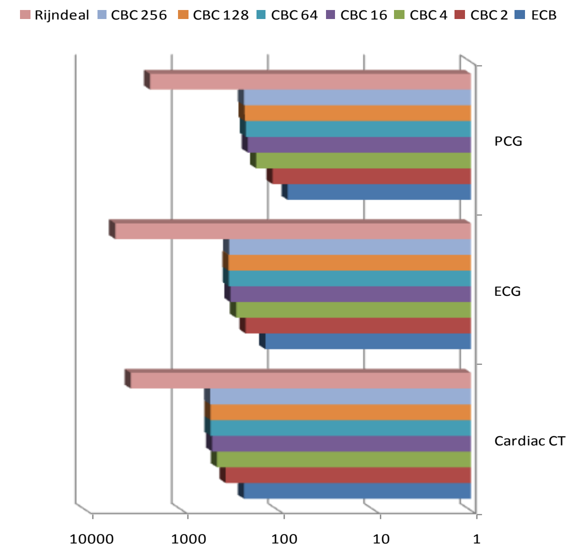
	Cardiac CT	ECG	PCG
Rijndeal	8.1	7.84	7.62
CBC 256	296.4	294.29	293.18
CBC 128	297.64	295.4	294.34
CBC 64	296.95	295.52	294.84
CBC 16	296.89	294.4	293.33
CBC 4	290.06	286.65	286.31
CBC 2	278.87	278.41	277.15
ECB	252.75	270.23	262.33

Fig. 24: Speed chart of different encryption methods.

4- 6 Noise sensitivity:

Noise sensitivity gain importance for event of the encrypted data transmission noise interference. A strong encryption method must have low noise sensitivity in addition to high security level and quality. The low noise sensitivity comes from resistance against noise in encrypted data. In cases of algorithm with high noise sensitivity the decrypted ciphertext contaminated by petty additive noise is useless and completely different with original data. To evaluate noise sensitivity, data is encrypted with aforementioned methods. A uniform random binary additive noise with 2% probability (or noise density) is applied to encrypted data. Noisy encrypted data is then decrypted. The error rate is calculated by MSE, MAE, SER and PSNR measures which are defined in (8), (9), (10) and (11) respectively. In these statements $P(i)$ and $P'(i)$ indicates original data and decrypted noisy encrypted data respectively. N indicates length of the entire data.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}[P(i) - P'(i)]^2 \qquad (8)$$



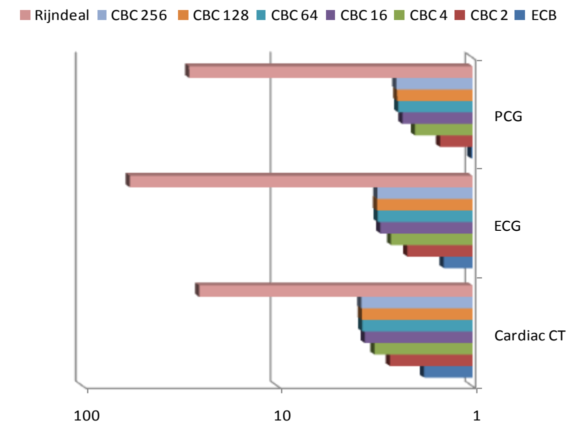
	Cardiac CT	ECG	PCG
Rijndeal	3468	5028	2176
CBC 256	516	329	230
CBC 128	513	333	226
CBC 64	512	331	220
CBC 16	494	319	210
CBC 4	439	278	172
CBC 2	357	221	116
ECB	230	138	81

Fig. 25: Mean square error of all encryption methods after adding equal error to encrypted data.

Mean Absolute error is similar to MSE except that in MSE small difference are understated and large difference are magnified, while in MAE there is no enlarging and lessening.

$$MAE = \frac{1}{N}\sum_{i=1}^{N}\left|P(i) - P'(i)\right| \quad (9)$$

Mean absolute errors are calculated regarding to (9) and are shown in a chart in Figure 26.



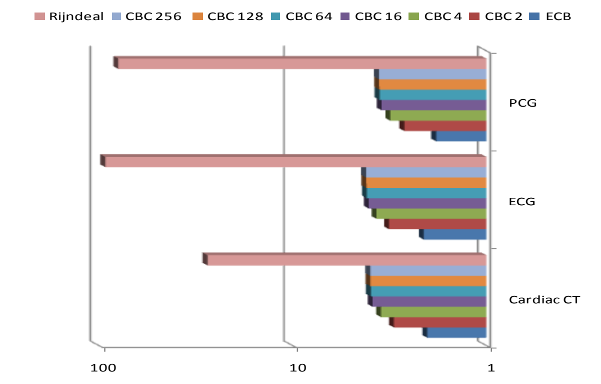
	Cardiac CT	ECG	PCG
Rijndeal	25.3497	57.4742	28.5342
CBC 256	3.7223	3.0767	2.4589
CBC 128	3.7011	3.0974	2.4382
CBC 64	3.6858	3.0716	2.4067
CBC 16	3.5773	2.9726	2.2887
CBC 4	3.1924	2.621	1.9748
CBC 2	2.6534	2.1623	1.4671
ECB	1.7747	1.4063	1.0147

Fig. 26: Mean absolute error of all encryption methods after adding equal error to encrypted data.

In digital data transmission, Symbol Error Ratio (SER) is considered a proper factor to evaluate the generated error percentage in each bit. SER indicates percentage of a symbols getting an error as consequence of additive noise.

$$SER = \frac{SymbolErrorNumber}{TotalNumberofSymbols} \times 100 \qquad (10)$$

Symbol error ratio of decrypted data is calculated by (10) and is shown as chart in Figure 27.



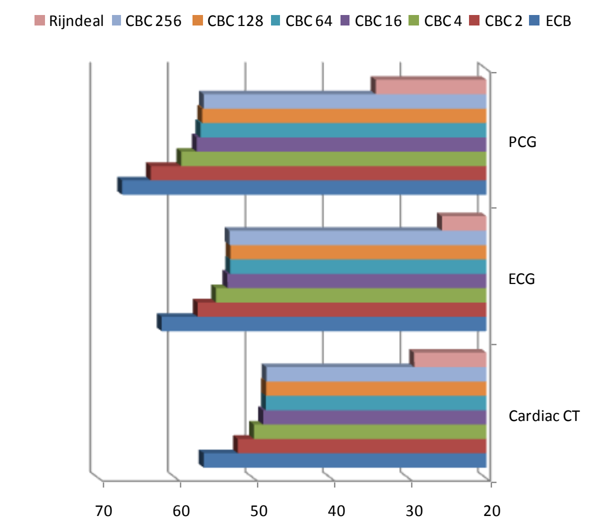
	Cardiac CT	ECG	PCG
Rijndeal	27.5252	92.6856	79.3811
CBC 256	3.9808	4.178	3.5876
CBC 128	3.9705	4.1687	3.5779
CBC 64	3.9509	4.1446	3.5608
CBC 16	3.8667	4.0495	3.4753
CBC 4	3.4983	3.6899	3.136
CBC 2	3.0012	3.1798	2.6538
ECB	2.0187	2.1047	1.8188

Fig. 27: Symbol error ratio of all encryption methods after adding same noise to encrypted data.

Peak signal to noise ratio presents maximum possible power of signal to power of destructive noise. The signal power usually covers a vast interval therefore it is usually measured in decibel[37].

$$PSNR = 10\log\left(\frac{\max(P)}{MSE}\right) \qquad (11)$$

Peak signal to noise ratio of all encryption methods is measured regarding to (11) and is shown as a chart in Figure 28.



	Cardiac CT	ECG	PCG
Rijndeal	29.3205	25.745	34.2925
CBC 256	48.3722	53.1482	56.4677
CBC 128	48.4359	53.0109	56.6519
CBC 64	48.4489	53.0552	56.8987
CBC 16	48.811	53.4162	57.3847
CBC 4	49.9836	54.8767	59.3766
CBC 2	52.0594	57.2454	63.2924
ECB	56.475	61.8883	66.9853

Fig. 28: Peak signal to noise ratio of all encryption methods after adding equal error to encrypted data.

As it was expected, all error measurements assign less noise sensitivity to OTP ECB method in comparison to OTP CBC mode.

It is observed that larger block size leads to higher noise sensitivity up to a certain amount.

Strong noise sensitivity of Rijndael is supported by all error measurements. The originated error from the decryption of noise data with Rijndael by MSE, MAE and SER measures are 25, 27 and 33 times higher than that of OTP CBC Mode.

The noise sensitivity for all encryption methods are demonstrated in Figure 29, it can be easily observed that OTP ECB Mode and Rijndael have lowest and highest noise sensitivity respectively.

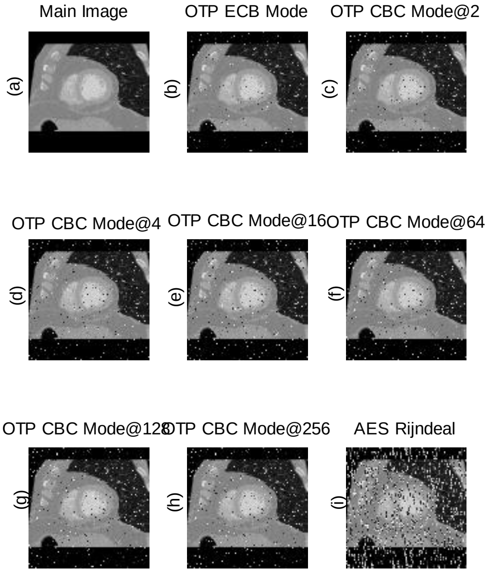


Fig. 29: A Cardiac CT slice image decryption after equally adding random noise; (a) The original image; (b) The encrypted image by OTP ECB; (c- h) Encrypted image by OTP CBC with different block size; (i) Encrypted image by Rijndael.

4-7 Key sensitivity:

The key sensitivity, which is relative to the key length, is of great importance in encryption. In Rijndael algorithm a key with 128-bit length is employed.

In OTP algorithms, assigned values to variable a, b, n, τ are 0.2, 0.1, 10 and 20 respectively. The initial value is set by a 32-bit float variable. To obtain more accurate initial value a 64-bit variable can be employed, although to preserve simplicity in this paper a 32-bit variable sets the initial value. The key length in OTP can vary between 32 and 208 bits, the minimum key length is chosen in this paper.

The key sensitivity is one of the critical features of a dominant encryption method. A small change in the key makes decryption impossible for a robust method.

In order to evaluate the key sensitivity a dataset is encrypted with KEY_1 and decrypted with KEY_2, which is different from KEY_1 only in one bit. Ideally a maximum difference between main data and decrypted data should be obtained by a wrong key.

To measure the difference between images again MSE, MAE and PSNR are applied. The strongest algorithm leads to the highest degree of difference and error, with a small modification in the key. In terms of key sensitivity the desirable result is to have maximum value for MSE and MAE and minimum value for PSNR.

In all encryptions by Rijndael the following 128-bit keys, which are different in the lowest value bit, are employed. The first key is applied for encryption and the second one for decryption.

KEY_1= 2B7E151628AED2A6ABF7158809CF4F3C
KEY_2= 2B7E151628AED2A6ABF7158809CF4F3B

All assessments in this section employed 32-bit keys as initial values of the Macky-Glass series. These keys are also different in the lowest value bit; the first key is applied for encryption and the second one for decryption[38].

KEY_1= $(3F99999A)_{Hex}$= $(1.2000000)_{Dec}$
KEY_2= $(3F99999B)_{Hex}$= $(1.2000002)_{Dec}$

Table 4 illustrates the MSE measure for original data and decrypted data with second key.

The chart in Figure 30 shows the MSE measure for Rijndael, OTP CBC Mode and OTP ECB Mode.

Table 4: Comparing OTP and AES methods' key sensitivity by MSE measure.

MSE	OTP ECB	OTP CBC 16	Rijndael
Cariac CT	12087	12087	15754
ECG	7,184	7,184	7,929
PCG	5,795	5,795	6,170

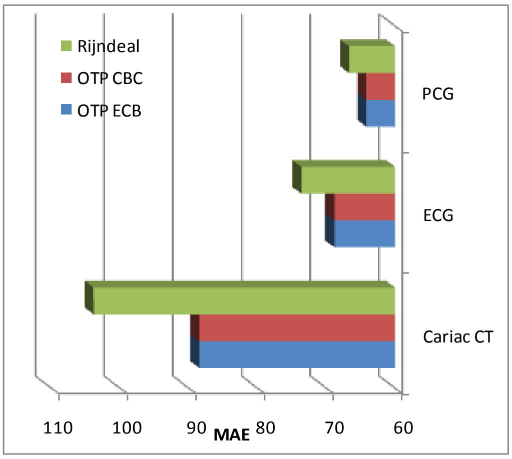


Fig. 30: MAE of original image and decrypted image with wrong key by Rijndael, OTP CBC Mode and OTP ECB Mode.

Figure 31 illustrates PSNR measure for original and decrypted data by Rijndael and OTP in both modes method with modified key.

According to the results, the key sensitivity for OTP in CBC and EBC mode is the same; and the key sensitivity for Rijndael is higher than that of OTP. Statistical analysis of error with MSE, MAE and PSNR measures indicates that Rijndael is more sensitive to key variation than OTP. Considering MSE and MAE measures Rijndael produces error 12.9% and 4.02% more than that of OTP, on the other hand Rijndael PSNR measure is 8.6% lower than that of OTP. However there is a slight difference between OTP and Rijndael, the statistical analysis support the powerfulness of Rijndael.

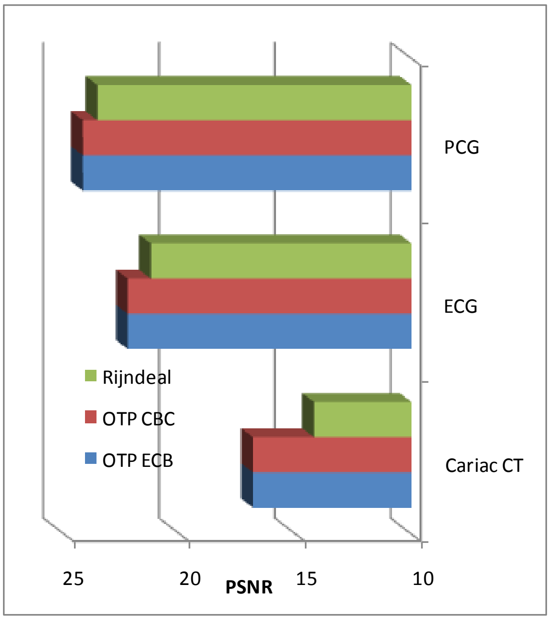


Fig. 31: MAE of original image and decrypted image with modified key by Rijndael, OTP CBC Mode and OTP ECB Mode.

Figure 32, represents logo3 image from Figure 15, and its decryption with the second key, after being encrypted by Rijndael and OTP methods.

From Figure 32 it can be easily inferred that even with small difference in key, OTP method preserve the image pattern covered up. While Rijndael reveals the image pattern which is Rijndael's weakness. Consequently it can be concluded that OTP for images with clear pattern is more key sensitive than Rijndael but this failure couldn't generalized for any other data types.

5. Conclusion:

In this paper an encryption method for medical data is proposed, which has acceptable security in addition to its unique easy implementation.

This method is compared by 7 factors with Rijndael encryption method, the most powerful encryption method available. In Table 5 result of this comparison are briefly stated.

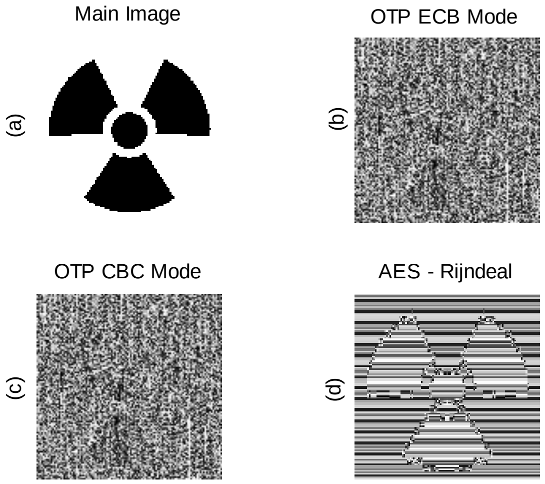


Fig. 32: (a) Original image; (b) OTP ECB Mode decryption with wrong key; (c) OTP CBC 16 Mode decryption with wrong key (d) Rijndael decryption with wrong key.

Table 5: AES and OTP encryption evaluation.

Method	OTP ECB	OTP CBC	Rijndael
EQ*	Highest	Intermediate	Intermediate
CCF**	Highest	Intermediate	Lowest
Histogram Spreading*	Low	Highest	Lowest
Pattern Hidding*	Lowest	High	Low
Spend Time**/ Throughput*	Low/ High	Lowest/ Hightest	High/ Low
Noise Sensitivity**	Lowest	High	High
Key Sensitivity*	Intermediate	Intermediate	High

* Higher is better, ** Lower is better

The proposed algorithm is faster, less noise sensitive and also better keeps the data pattern hidden in comparison to Rijndael method.

It is a uniquely simple procedure, with an easily possible hardware implementation by logic gates and 8-bit microprocessors.

References

1. Mustapha Machkour, Y.I. Khamlichi, K. Afdel, 2006. Data security in medical information system. International Conference on Multimedia Computing and Systems; ICMCS '092006. p. 391-4.
2. Kovacevic, S., M. Kovac, J. Knezovic, 2007. System for Secure Data Exchange in Telemedicine. 9th International Conference on Telecommunications; ConTel 20072007. p. 267-74.
3. Jacob Andersen, B. Lo, G.Z. Yang, 2005. Experimental Platform for Usability Testing of Secure Medical Sensor Network Protocols. 5th International Summer School and Symposium on Medical Devices and Biosensors; ISSS-MDBS 20082005. p. 179-82.
4. Lin, C.C., P.Y. Lin, P.K. Lu, G.Y. Hsieh, W.L. Lee, R.G. Lee, 2008. A healthcare integration system for disease assessment and safety monitoring of dementia patients. IEEE Trans Inf Technol Biomed., 12(5): 579-86.
5. Tanenbaum, A.S., 2003. Computer Networks. 4 ed: Prentice Hall.
6. Kaufman, C., R. Perlman, M. Speciner, 2002. Network security: private communication in a public world: Prentice Hall Press.
7. Kahate, 2008. Cryptography and network security: Tata McGraw-Hill Education.
8. Dünnebeil, S., F. Köbler, P. Koene, H. Krcmar, J.M. Leimeister, 2011. Encrypted NFC emergency tags based on the German Telematics Infrastructure Third International Workshop on Near Field Communication 20112011.
9. Yu, W.D., V. Jothiram, 2007. Security in Wireless Mobile Technology for Healthcare Systems 9th International Conference on Digital Object Identifier.
10. Gilmore, J., 1998. EFF builds DES cracker that proves that data encryption standard is insecure. EFF press release.
11. Daemen, J., V. Rijmen, Proposal A. Rijndael, 2011.
12. Gladman, D.B., Rijndeal (by Joan Daeman & Vincent Rijmen), 2003. A Specification for the AES Algorithm, 15.
13. Vernam, G.S., Secret signaling system. Google Patents; 1919.
14. Kahn, D., 1996. The Codebreakers: The Story of Secret Writing, revised ed. New York: Scribner.
15. Shannon, C.E., 1949. Communication Theory of Secrecy Systems*. Bell system technical journal, 28(4): 656-715.

16. Molotkov, S.N., 2006. Quantum cryptography and VA Kotel'nikov's one-time key and sampling theorems. Physics-Uspekhi, 49(7): 750-61.
17. Chen, Z., J. Xu, 2008. editors. One-Time-Pads encryption in the tile assembly model. Bio-Inspired Computing: Theories and Applications, 2008 BICTA 2008 3rd International Conference on: IEEE.
18. Zhang, Y., C. Xu, F. Wang, 2009. editors. A novel scheme for secure network coding using one-time pad. Networks Security, Wireless Communications and Trusted Computing, 2009 NSWCTC'09 International Conference on: IEEE.
19. Lindquist, T.E., M. Diarra, B.R. Millard, 2004. editors. A java cryptography service provider implementing one-time pad. System Sciences, 2004 Proceedings of the 37th Annual Hawaii International Conference on: IEEE.
20. Han, F., J. Hu, K. Xi, 2010. editors. Highly efficient one-time pad key generation for large volume medical data protection. Industrial Electronics and Applications (ICIEA), 2010 the 5th IEEE Conference on IEEE.
21. Ishawy, N.E.F., O.M.A. Zaid, 2007. Quality of Encryption Measurement of Bitmap. Images with RC6, MRC6, and Rijndael Block. Cipher Algorithms. International Journal of Network Security & Its Applications (IJNSA), 5(3): 241-51.
22. Jeyamala, C., S. GopiGanesh, G. Raman, 2010. editors. An image encryption scheme based on one time pads-A chaotic approach. Computing Communication and Networking Technologies (ICCCNT), International Conference on: IEEE.
23. Ahmed, H.E.d.H., H.M. Kalash, O.S.F. Allah, 2007. An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption. Informatica (Slovenia), 31(1): 121-9.
24. Wu, Q., Y. Cao, 1995. editors. An equivalent stochastic system model for control of chaotic dynamics. Decision and Control, 1995, Proceedings of the 34th IEEE Conference on: IEEE.
25. Wang, D., J. Yu, 2008. editors. Chaos in the fractional order Mackey-Glass system. 2008 International Conference on Communications, Circuits and Systems.
26. Kyrtsou, C., M. Terraza, 2003. Is it possible to study chaotic and ARCH behaviour jointly? Application of a noisy Mackey–Glass equation with heteroskedastic errors to the Paris Stock Exchange returns series. Computational Economics, 21(3): 257-76.
27. Moody, G.B., R. Mark, 1992. MIT-BIH arrhythmia database directory. MITBIH Database Distribution, Harvard–MIT Division of Health Sciences and Technology, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA Available on the World Wide Web at:(http://www physionet org/physiobank/database/html/mitdbdir/mitdbdir htm)(last date visited: Jul 23, 2008).
28. Rangayyan, R.M., 2002. Biomedical signal analysis: IEEE press New York.
29. Milad General Hospital Isfahan, Iran. Available from: http://www.isfahanmiladhospital.ir/e-n/.
30. SOMATOM Sensation, Siemens AG: 2002-2011. Available from: http://www.medical.siemens.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=1&catTree=12781&langId=1&productId=143945&storeId=10001.
31. Ahmed, H.E.d.H., H.M. Kalash, O.S.F. Allah, 2007. Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images. International Journal of Computer and Information Engineering, 1(1): 33-9.
32. Elkamchouchi, H., M. Makar, 2005. editors. Measuring encryption quality for bitmap images encrypted with rijndael and KAMKAR block ciphers. Radio Science Conference, 2005 NRSC 2005 Proceedings of the Twenty-Second National: IEEE.
33. Ziedan, I.E., M.M. Fouad, D.H. Salem, 2003. editors. Application of data encryption standard to bitmap and JPEG images. Radio Science Conference, 2003 NRSC 2003 Proceedings of the Twentieth National: IEEE.
34. Ahmed, H.E.d.H., H.M. Kalash, O.S.F. Allah, 2006. Encryption quality analysis of the RC5 block cipher algorithm for digital images. Optical Engineering, 45(10): 107003-7.
35. Krishnamurthy, G., D.V. Ramaswamy, 2008. Encryption quality analysis and Security Evaluation of Blow-CAST-Fish using digital images. Communicated to International Journal of Computational Science.
36. Krishnamurthy, G., V. Ramaswamy, 2010. Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images. arXiv preprint arXiv:10040571.
37. Huynh-Thu, Q., M. Ghanbari, 2008. Scope of validity of PSNR in image/video quality assessment. Electronics letters, 44(13): 800-1.
38. Krishnamurthy, G., V. Ramaswamy, M.G. Leela, 2007. Performance Enhancement of Blowfish algorithm by modifying its function. Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications: Springer, pp: 241-4.