A New Medical Images Encryption algorithm Based on Gold Code: Futures Trends Towards Telemedicine

A New Medical Images Encryption algorithm Based on Gold Code: Futures Trends Towards Telemedicine

Mohammad H. Ellewe
Junior Master Student, University of Anbar,College of Computing and Information Technology,Dept. of Computer Science, Iraq
E.mail:mo.no.ja87@uoanbar.edu.iq

Ali M. Sagheer
Al-Qalam University College
E.mail: ali.m.sagheer@gmail.com

Azmi Shawkat Abdulbaqi
University of Anbar,College of Computing and Information Technology
Dept. of Computer Science, Iraq
Email: azmi_msc@yahoo.com
azmi_msc@uoanbar.edu.iq

Abstract

The rising necessity for telemedicine has made the healthcare sector an urgent and unlimited necessity to secure important data sent between medical centers for treatment purposes. The medical image encryption is a significant technique to attain a medical images security (MIS). There are numerous researchers utilized advanced encryption standard (AES) to guarantee of MIS. The direct application of AES encryption technology on medical images led to a long-time of processing; also it leads to a clear background regions, which are considered defects. This article includes the application of information theory (IT) to detect regions of the medical image that include, ROI (regions of interest) and ROB (regions of background). To reduce processing time and protect the medical image by utilizing AES with a higher degree of protection, a hybrid encryption is applied to ROI, and a method of coding such as gold code (GC) is applied to ROB after creation. The proposed method involves less time processing for the entire medical image of the AES application and has the best possible security as described in the entropy and link calculations.

Keywords: Information Theory (IT); Medical Image Encryption; Gold Code (GC); Advanced Encryption Standard (AES); Entropy.

1. Introduction

Medical images transmission between center of medical database to the remote radiologist center without applying security methods leads to a low-level privacy for patients. The necessity to employ the security techniques for medical images has increased with the technologies utilization of telecommunications for medical diagnosis and patients care when the client and the provider are separate by distance, in a system known as telemedicine.

Telemedicine is significant due to it allows remote specialists consultations, loss-free and to reaches to the patient's medical information immediately, and enhanced communication between patients and specialists in a healthcare system. This procedure leads to medical care quality improvement, and easy access to the medical databases, from which medical images can be either stored or transmitted through a channel to destination (specialists).

Many researchers was suggested an AES encryption technique for secure the medical data transmission[1].

The AES technique implementing for a medical image takes a long processing time. For example, and based on computer has CPU Intel Core2 Quad Q6700, to encrypt 512×512 pixels of MRI brain image, it need to 521.67 second. To solve this obstacle, there are several tried by researchers utilizing a selective-encryption to encrypt any parts of the image [3] [4] or image pixels parts [5] in order to decrease the time of the processing, but this solution reduce the security level. In addition, there is a robustness problem even by applying AES for the whole medical image [6]. Figures 1 and 2 display some of the difficulties.

2. Background and Related Works

2.1 MIE Considerations

There are several important considerations was presented below used to design encryption schemes for medical data application purposes [7]:

2.2The Size of Data:

Due to lossless compression the size of the medical data is massive. Some current ciphers' speed of encryption/decryption (EN/DC) isn't fast enough, particularly software implementations that utilize the naive method. Consequently, the quantity of data to be encrypted is an important aspect of medical imaging systems.

2.3 Compressibility:

After encryption, when the process of the compression is performed, the randomness encrypted test achieves a significant reduction in the amount of compression when the compression is performed after encryption. According to that, one common method is to content encryption after compression, however, compressed content must be fully encrypted after compression. Therefore, a particular stage within the compression step that can be partially encrypted is calculated without affecting the compression cycle. Thus, a trade-off between compression and encryption is required.

2.4 The Property of Avalanche:

To demonstrate that the utilized algorithm in the encryption process is perfect, it must have avalanche property, since a major change in the ciphertext must take place with a slight change to the plain text or key.

2.5 Security-Measures and Accessibility:

There are high-security measures related to the production of a strong and ideal encryption algorithm capable of producing an encrypted text that has the ability to resist various attacks if it comes to keeping medical image samples for a long time.

B. The various MIE techniques encryption algorithms

The various MIE techniques encryption algorithms can be collected of substitution techniques, transposition techniques or both. In substitution techniques, the values of pixel of

the plaintext image are replaced by new values, while in transposition techniques, the values of pixel of the plaintext image are repositioned in a new sequence.

The medical imaging encryption algorithms can also be classify into two categories according to the applied pixels; these approaches are naive and selective encryption. The naive approach is utilized for all image pixels encryption. The selective encryption is utilized for selected image pixels encryption.

There are several criteria by which to determine the robustness of the safety of the cipher technology mathematically:

1) The breaking- cipher-cost exceeds the true value of the encrypted information.

2) The required time for cipher-breaking more than the beneficial information lifetime.

The naive method is easy to implement, but all pixels must pass via the EN/DC stages. On the other hand, the selective type of encryption is more complicated to implement, but the processing time is shorter because the pixels specified are subjected to the EN / DC stages only. As an example of the naive method is the chaotic maps proposed for securing medical images like "Cat maps" or "Baker maps"; the method has a short implementation time but it can be broken within a short time.

3. Gold Code Sequence

Gold Codes (GC)(also called Gold sequence), are a kind of binary string (string of 0's and 1's) . It is usually utilized in communications systems such as CDMA, CDMA (GPS) and cell phones. GC are named by Dr. Robert Gold in 1967. It features a easy to generate by HW or SW, and have features resembling random noise. GC based on XOR and Shift registers.

There are small cross-correlations in a group identified by the GC. These correlations are of great value when different devices broadcast their signals in the same frequency range.

4. Coding Based Security Purpose

There are numerous coding algorithms like "Gold" and "Kasami" that utilized for image encryption. In [9] Gold code algorithm, for the first time and for network security, this algorithm was utilized to encrypt data. However, the Gold code algorithm can be amended to be utilized for medical images. The Gold code algorithm is based on a pseudo-noise sequence generator. It is a very beneficial and effective code due to a great number of codes that can be providing by its generator. Practically, they are created by a module 2 addition of a pair of maximal equal length code sequences. Bit by bit are added with synchronous clocking. Based on Figure 3 which illustrates the schema of simple scrambling code generator circuit where code 3 represents the Gold code output. The signal encoding type does not increase the signal redundancy that fixes the dilemma between data compression and data encryption due to the increased efficiency of encoded signal compression.

The chaotic sequence utilization will enhance the code performance for image applications [10]. It should be noted that n registers generator can generate a length sequence (Ls) equal to:

$$L_s = 2^n - 1 \qquad (1.1)$$

The figure 1 below, displays the simple diagram of Gold Cold Generator.

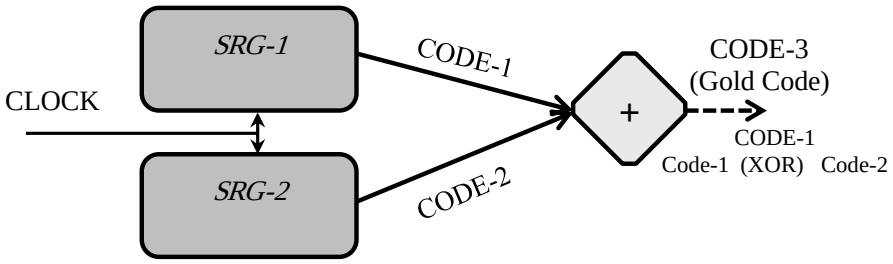


Fig. 1. Gold Cold Generator Diagram

In this presented scientific material, a new encryption technique based on utilizing three Gold codes (3GC) and it is significant to choice the appropriate length for everyone, was designed. The Gold code-1 length (LG-1) should be more than 2/3 of the image dimension x depth of pixel. Gold code-2 Length (LG-2) depends on the number of bits that intended to replace some bits in Gold code-1. Thus, the minimum length should be (LG-1/depth of the pixel) x number of replacing bits in the pixel. Gold code-3 length (LG-3) should be more than (LG-1/depth of the pixel) x number of bits indicating the replacement position.

Gold codes are very sensitive where the change in the starting point, feedback connections, or any frame bit will change the output values that are XORed with the pixels of the image.

Figures 2 and 3, displays the block diagrams of the suggested encryption technique for ROB based on Gold code-1 and Gold code-2 bits respectively; in case a the probability of changing the pixel value is 50% while the probability in case b is 75%. This technique could be expanded to more than two Gold codes where a multiplexer controlled by another Gold code will produce the output encryption code.

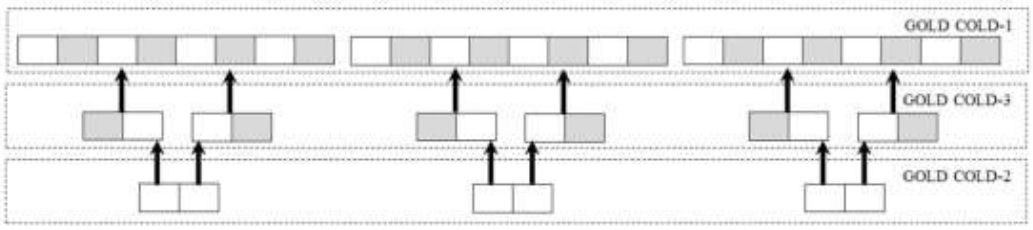


Fig. 2. The Proposed of Encryption Code (Replace One Bit)

5. Information Theory Based Medical Image Segmentation

Medicinal images are distinct from another images due to they have their own characteristics. There are two regions to represent medical images, one is the part that represents the informative part is called the regions-of-interest (ROI), and the other is the part that represents the non-informative part called non-region-of-interest i.e Regions-of-background (ROB).

Based from that point of view, a high-performance encryption technique in the implementation time and power consumption, where the segmentation method explains the utmost appropriate method to locate the areas of ROI and ROB exactly. Segmentation is the process of testing whether every pixel belongs to an ROI or ROB upon some parameters like the threshold value and creates a binary-image where the pixel has a single value equal 1 if this pixel belongs to the ROI; otherwise, it is 0. After the segmentation process is completed, the medical picture is divided into several areas, and the boundaries between these areas become known.

There are three main types of segmentation algorithms that are utilized for medical image segmentation: threshold algorithms, pattern recognition techniques, and distorted models [11]. In this article, the entropy-based threshold segmentation technique was utilized. The threshold techniques types can be classified into pixel-based techniques, where gray values are utilized for individual pixels only, edge-based techniques by edges detecting and recognition, and then attempting to follow them, and area-based techniques by analyzing gray values in large areas. However, the entropy utilized to segment the medical images can provide a preferable performance than other traditional techniques due to the decision depends on the density of information in pixels, not on the pixel density itself. In this article, the recognition of both ROI and ROB is based on the information theory where entropy is utilized to each region recognize based on its information. This technique gives the best outcomes than basic segmentation techniques to recognize the region. Entropy can be defined as the statistical measure of randomness and disturbance where En(d) is measured from data d according to the following equation [12]:

$$E_n=\sum_{i=1}^{L} p(m_i)\log\frac{1}{p(m_i)} \quad (2)$$

where L referred to pixel values number and p(mi) indicates the occurrence probability of a pixel with value mi. Note that , the histogram is considered to sufficiently uniform if the encrypted image entropy of is closer to log L bits.

6. Image Evaluation techniques

In order to check the performance and efficiency of the new algorithm, this algorithm is analyzed depending on the main features and general characteristics of the medical image. For example, the average image can be explained as the pixel value average of an image. In the grayscale medical images, they are equivalent to the average brightness or intensity, whilst, the spread of pixel values nearly the medical image is average, in the image contrast.

1. Histogram

Based on the encrypted image, the utilization of its diagram should be closer to the uniform distribution in order to prevent the statistical attacks [12]. The medical image histogram shows the number of iterations for each gray level. Arithmetically, the graph is a separate function and its gray levels are in the range [0, L - 1] as in the following equation:

$$\text{hist}(rk) = \frac{nk}{N} \quad (3)$$

where N shows to overall pixels number in the image, and rk indicates to kth gray level and nk Indicates the pixel number of the medical image in that gray level. The histogram allows a global description of the image. Therefore, when the medical image is not visible, this indicates that the narrow histogram due to the number of gray levels in the medical image is low. Conversely, if the histogram is widely distributed, it indicates that there are all lead-gray levels in the inserted medical image. Thus, in general, the contrast and vision ratio in medical images is increased[13].

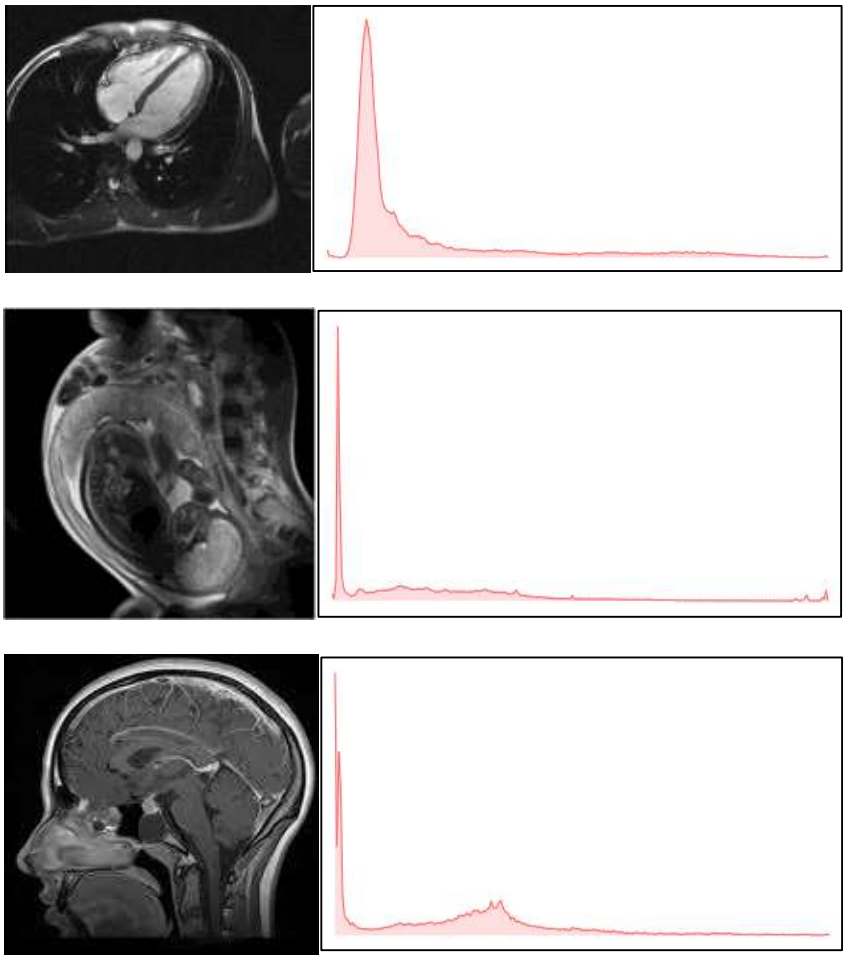


Fig. 3. Images Histograms

2. Correlation Coefficient

An important characteristic of a medical image encryption algorithm is its resistance to statistical attacks when the pixel correlation coefficients in the encrypted image are as low as possible. The calculation of diagonal, vertical, and horizontal correlation coefficients (rxy) of two adjacent-pixels utilizing the following equation[14]:

$$\mathrm{Cor}_{xy} = \frac{\mathrm{COV}(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \quad (4)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{i=1}^{N} x_i) \quad (5)$$

$$\mathrm{COV}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - \mathrm{Av}(x)\big)\big(y_i - \mathrm{Av}(y)\big) \quad (6)$$

x and y indicates to the two adjacent-pixels of gray-scale values in the image, and Av indicates the average value that shown in the following eq.

$$\mathrm{Av}(z) = \frac{1}{N}\sum_{i=1}^{N} z_i \quad (7)$$

Based on the encoded image, there are about a thousand pairs of two adjacent-pixels (diagonal, random, and horizontal) randomly chosen, and randomly calculate and the correlation coefficients are randomly calculated and consecutively.

3. The discrepancy between Plain and Encrypted Images

So as to overcome the encrypted text attacks, the original image must be significantly different from the entire encrypted image. To achieve this requirement, three basic measures are used: number of pixel change units (NPCR), absolute mean error (MAE), as well as average variable intensity of change (UACI)[13]. Each stage of the difference between encrypted images and plain images is measured by the mean absolute error (MAE), where indicate (L) the size of the image. aij and bij indicates to the pixels grayscale values of plain-images and encrypted images, respectively. The NPCR is the percentage of corresponding pixels with different gray levels in two images. Let C1(i, j) and C2(i, j) be the gray level of the pixels at the ith row and jth column of two (W × H) images. The NPCR of these two images is defined in [14].

$$\mathrm{NPCR} = \frac{\sum^{i,j} D(i,j)}{W \times H} \times 100\% \quad (8)$$

D(I,j) can be defined as a follow:

$$D(i,j) = \begin{Bmatrix} = 0, \text{if } C_1(i,j) = C_2(i,j) \\ = 1, \text{if } C_1(i,j) \neq C_2(i,j) \end{Bmatrix}$$

7. The Proposed Algorithm

The propose algorithm is shown in Figure 6, and the steps for both EN/DC are illustrated below.

1. Encryption

- The medical image is divided into many blocks.
- The correct selection of initial conditions AES as well as the Gold code.
- Entropy is applied to the medical image to recognize ROI and ROB where the result is two vectors, one white and one black respectively.
- ROI vector is encrypted using AES.
- ROB is encrypted using Gold code.
- The image is reconstructed using the stored black and white image.
- The edges that might result from the previous step could be removed by applying another round of Gold code or by using any chaotic method such as cat map.
- The uncolored image (black and white image) is compressed utilizing any compression technique such as Huffman encoding to get a small file with encrypted medical image sent as a key.

2. Decryption

The needed keys for decryption are:

1. Keys of AES used to encrypt ROI.
2. Parameters and initial conditions for the Gold code used to encrypt ROB such as the shift of the code and the code level.
3. The compressed file of the black and white image. Decryption steps are:

- The received encrypted medical image is read.
- The permutation algorithm is used.
- The two regions are separated using the compressed file, resulting in two vectors representing ROI and ROB.
- The ROI vector is decrypted using AES and ROB vector using Gold code.

- The image is reconstructed using the received file that contains the black and white image.

3. Results and Discussion

In this article we reduced encryption processing time for medical images using partial encryption. The proposed algorithm uses image segmentation based on information theory technique. Medical images shown in Figure 7 are utilized and segmented using entropy as presented in Figure 8. Table I displays the ratios of ROI and ROB to confirm the efficiency of the suggested algorithm. The ratio of ROI is less than 75%, therefore encrypting ROI using AES only saves 25% of the processing time.

Table II displays the processing time needed for medical images encryption utilizing the source code in [8] utilizing a computer runs on a Intel CPU type Core i5. Figure 9 and Table III display a comparison between AES and Gold code when encrypting a piece of ROB, where Gold code has a better performance than AES except in NPCR parameter. Figure 10 displays steps for the encryption algorithm when applied to a medical image.

Table 1. indicates to ROI and ROB ratio in three types of Medical Images.

Tested Medical Image	Image Size	Total Image Pixels	ROI	ROB	ROI%	ROB%
Brain Image Size	380×367	135360	96064	39296	70.97	29.03
Womb Image	504×384	193536	120247	73289	62.13	37.87
Heart Image	496×480	238080	80000	158080	33.60	66.40

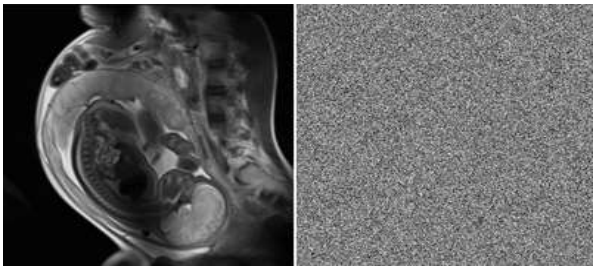
Table 2. indicates to the Time of AES Encryption Processing

Medical Image Type	Medical Image Size	Medical Image Dimension	The Processing Time
Brain Image	18.3 Kb	336×336	420.2153 s
Heart Image	15.1 Kb	144×144	73.7856 s
Womb Image	11.7 Kb	352×352	470.0156 s

Table 3, indicates to the Time of AES Encryption Processing Based Two Entropies

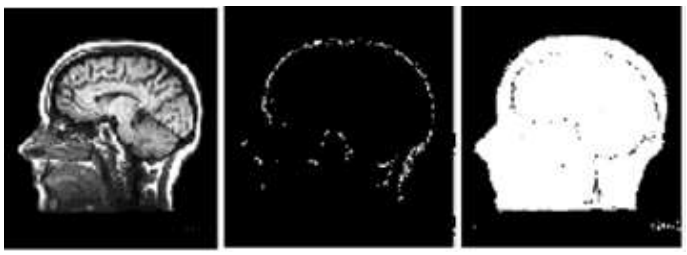
Medical Image Type	Image Entropy	Correlation	NPCR
AES Encryption	2.6539	0.0073	1
GC Encryption	3.2908	0.0047	0.9062

The below figure explain the original womb mage and the encryption image.



(a) (b)

Fig. 4. (a) Original Image (b) Encrypted Image

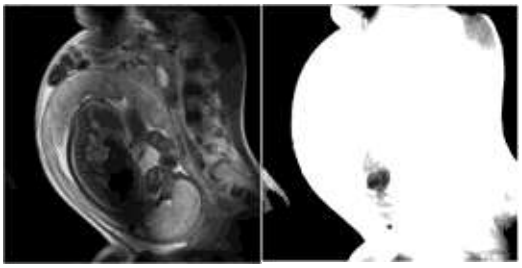


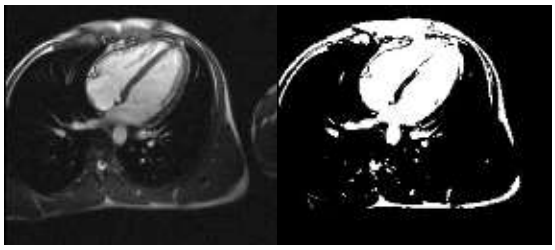
(a) (b) (c)

Fig. 5. (a) Original Brain Image MRI, (b) MRI Brain Image with threshold=0

(c) MRI Brain Image with threshold=255

(a)





(c)

Fig. 6. (a) , (b), and (c) Entropy Based Brain Image Segmentation

4. Conclusion

Encrypting a medical image using AES method offers a high degree of security, but encryption of the entire image takes a long time to implement. Assigning short keys for AES leads to problems in the ROB, and assigning longer keys means longer processing time. Whilst work has demonstrated that partial encryption is a reasonable solution to this problem, we look at this issue from a new point of view: Medical image segmentation can be used and AES applied only to protect the ROI field, with another encryption technique that shortens the

ROB processing time. The ROB might be left before encryption, but it is easier to encrypt ROB with any information that could be considered as watermarked in this area. The ratio of the ROB is varied; still, it is more than 25% of the total image. The processing time in our method will be reduced. The information theory is also utilized to implement the segmentation process, which gives more accurate outcomes than segmentation techniques based on the intensity of the pixel. Additionally, a new encryption algorithm based on the GC was designed and utilized due to it has the ability to withstand various attacks.
In order not to be exposed to brute force attack and for the purpose of reducing the possibility of breaking the coding method, the 3GC was incorporated. As well as, the starting bit of the code can vary and therefore be considered an additional key. Two-regions mixing utilizing a permutation technique like a cat map will eliminate any information that distinguishes these regions, and increasing the strength of the suggested technique. The transmitted file size that results from the segmentation process is very small because having only black and white images, and a file is easily compressed in a lossless method with any compression technique.

References

[1] N. E. M. Association, "Digital Imaging and Communications in Medicine (DICOM) Part 15: Security and System Management Profiles," available online athttp : //medical.nema.org/dicom/2004/0415PU.PDF, 2004.
[2] Y. Zhou, K. Panetta, and S. Agaian, "A lossless encryption method for medical images using edge maps," in Proceedings of the 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society: Engineering the Future of Biomedicine, EMBC 2009, Minneapolis, MN, 2009, pp. 3707 – 3710.
[3] Y. Ou, C. Sur, and K. Rhee, "Region-based selective encryption for medical imaging," in Proceedings of the 1st annual international conference on Frontiers in algorithmics. Springer-Verlag, 2007, pp. 62–73.
[4] Z. Brahimi, H. Bessalah, A. Tarabet, and M. Kholladi, "Selective encryption techniques of jpeg2000 codestream for medical images transmission," WSEAS Transactions on Circuits and Systems, vol. 7, no. 7, pp. 718–727, 2008.
[5] R. Norcen, M. Podesser, A. Pommer, H. Schmidt, and A. Uhl, "Confidential storage and transmission of medical image data," Computers in Biology and Medicine, vol. 33, no. 3, pp. 277–292, 2003.
[6] M. Ashtiyani, P. Birgani, and H. Hosseini, "Chaos-based medical image encryption using symmetric cryptography," in Proceedings of the Inter- national Conference on Information and Communication Technologies from Theory to Applications - ICTTA'08, Damascus, Syria, 2008, pp. 2781 – 2785.
[7] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J. Quisquater, "Overview on selective encryption of image and video: challenges and perspectives," EURASIP Journal on Information Security, vol. 2008, pp. 1–18, 2008.
[8] J. Buchholz, "Advanced Encryption Standard," available online at buchholz.hs-bremen.de/aes/aes.htm, 2001.
[9] A. Jabbar and A. B. Mahmood, "Analysis and design of a novell vpn switch," Al-Rafidain engineering journal, vol. 13, no. 4, pp. 11 – 25, 2005.
[10] M. Youssef, M. Zahara, A. Emam, and M. Elghany, "Image encryption using pseudo random number and chaotic sequence generators," in National Radio Science Conference, NRSCl, New Cairo, Egypt, 2009, pp. 1–15.
[11] Z. Ma, J. Tavares, and R. Jorge, "A review on the current segmentation algorithms for medical images," in IMAGAPP 2009. First International Conference on Imaging Theory and Applications, Lisboa, Portugal, 2009, pp. 135 – 140.
[12] K. Wong, "Image Encryption Using Chaotic Maps," Intelligent Comput- ing Based on Chaos, pp. 333–354, 2009.
[13] Y. Mao and G. Chen, "Chaos-based image encryption," Handbook of Geometric Computing, pp. 231–265, 2005.
[14] E. Shahram and E. Mohammad, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm," Mathematical Problems in Engineer- ing, vol. 2009, pp. 1–22, 2009. 601