International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Medical Image Encryption Using Modified AES

Woud Majid Abed, M.Sc.

Lecturer at the Department of Basic Science, College of Dentistry, University of Baghdad, Iraq

Abstract: ***In recent years mostly all the health centers and hospitals use the wireless networks and internet for biomedical information exchanging, the secure of this information in not verified and cannot be grantee in such environment, the personality of patient and for security concerns inside such institutions there is a need for encryption system that can easily encrypt the biomedical data and it can be shared with other centers via internet without and concerns about privacy. Our system based on modified advanced encryption standard (AES), with encryption and decryption in real time taking to consideration the criticality of data that been encrypted.***

Keywords: Advanced encryption standard, AES, Medical image encryption, modified AES

1.Introduction

Advanced encryption standard (AES) is consider one of the popular block ciphers worldwide, many attacks is formed in AES, none of these attacks can totally cryptanalysis this algorithm, the modification suggested to this algorithm goal is to improve the security offered by it and add randomness to original algorithm [1].

Medical image security is very important issue in new world technologies with the internet of things (IOT) revolution everything is connected to the internet and need to protected and authenticated [2], our proposed system can encrypt the medical images for popular people or the critical situation patient that can help to protect the patients privacy by merging many techniques, the modification of AES algorithm can be performed by adding the A5/1 keystreams generating algorithm, the keystream generated by this algorithm enter the AES system to generate the AES key schedule.

In [3] A5/1 algorithm is modified to overcome the weaknesses that can appear in majority function by mixing new s-box techniques to the algorithm and the number of LFSR is changed to 5, the randomness is improved and the time consideration is still in the real time application accepted levels, this proposed algorithm sued in our system to generate key stream that is used in AES key generating.

A5/1 Algorithm [4]

The algorithm that generates the key stream in global system for mobile communication, three linear feedback shift register is used in this algorithm with (19, 22, and 23) number of registers respectively the following equation that is used in each LFSR, see table (1), and figure (1).

Table 1: A5/1 equations, clocking and tapped bits

LFSR number	Length in bits	Feedback polynomial	Clocking bit	Tapped bits
1	19	$x^{19}+x^{18}+x^{17}+x^{14}+1$	8	13, 16, 17, 18
2	22	$x^{22}+x^{21}+1$	10	20, 21
3	23	$x^{23}+x^{22}+x^{21}+x^{8}+1$	10	7, 20, 21, 22

This algorithm generates 228 bits by accepting 64 bit session key and 22 frame numbers.

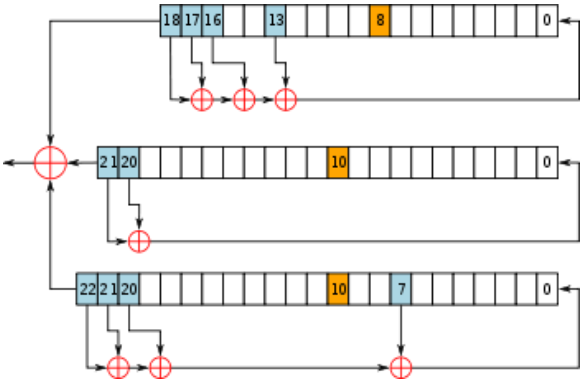

Figure 1: A5/1 structure [4]

2.Advanced Encryption Standard

AES block cipher can be implemented with many bits size (128,192 and 256 bits) each 128 bit is divided to mainly four blocks of operations that are applied on (4*4) matrix that is known as (state) the number of rounds is different according to the number of bits (10 rounds for 128 bits, 12 round for 192 bits and 14 round of 256 bits) each round is consist of four basic transformation [5].

1. S-box transformation: using special table called s-box that is use for substitution operation and s-box inverse table; these bytes will be replaced with others by using the lookup table (s-box), non linearity can be granted by this step, as shown figure (2)[5].

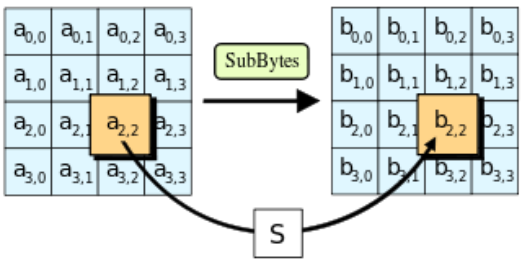

Figure 2: s-box [7]

2. Shift rows: simply this operation is transposition of bytes, by applying cyclic shift operation for the last 3 rows, row number two shifted only one byte and row number three shift two bytes and row number four shift three bytes. As shown figure (3) [6].

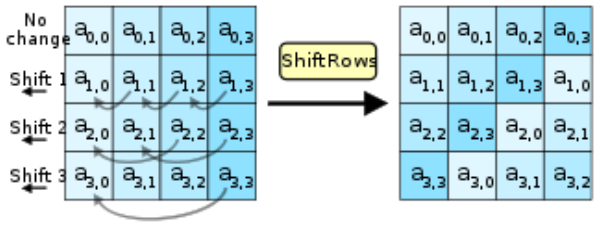

Figure 3: Shift rows [7]

3. Mix column: the columns of vector always multiplied by the value of fixed matrix (see table 2) the bytes in this step is treated as polynomials equations. As shown figure (4)[6].

Table 2: Fixed matrix (mix column)

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

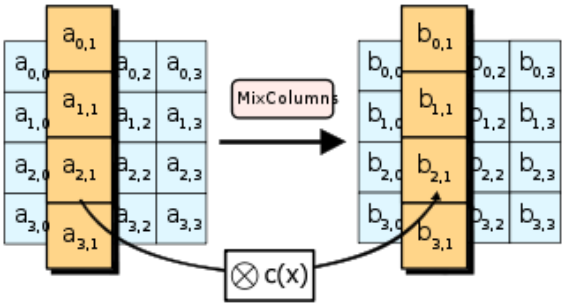

Figure 4: Mix columns [7]

4. Add round key: The XOR operation between the round key and the resulted state. As shown figure (5) [7].

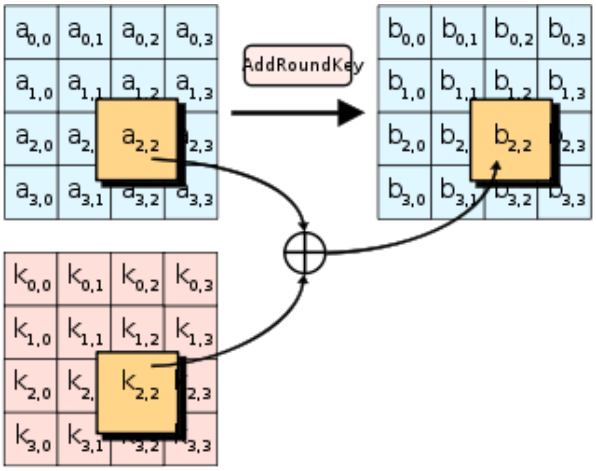

Figure 5: Add round key [7]

3.Proposed System

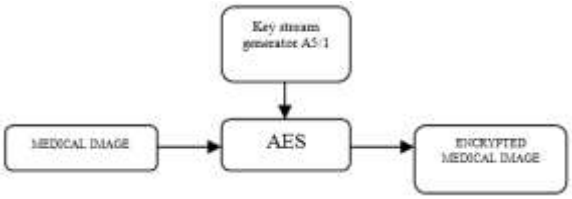

Figure 6: Proposed system

The modified advanced encryption standard (AES) that can be obtained by merging one of keystream generating methods (i.e. modified GSM keystream algorithm A5/1), the key obtained by this methods maximize the randomness of the key and add more level of security to the proposed system.

The test operation of AES algorithm is done via software application different samples images were tested and used; the time needed for encryption operation is shown in table 3 with the two samples image dimensions.

Table 3: Samples medical image used details

Sample name	Dimensions	Time to Encrypts
Sample 1	750 * 422	14 s
Sample 2	265 * 190	02 s

Figure 7: Medical image sample 1

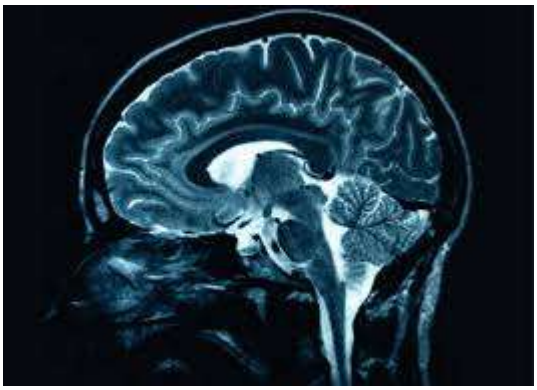

Figure 8: Medical image sample 2

Each sample is encrypted and decrypted with the proposed system independently and the following encrypted data is the result. Figure (9, 10)

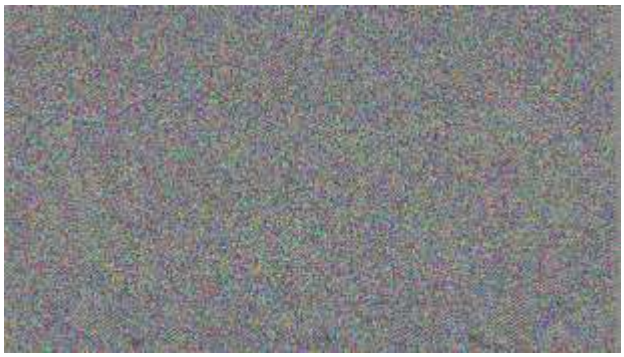

Figure 9: Sample 1 encrypted image

Figure 10: Sample 2 encrypted image

The histogram and entropy is calculated for both samples original image and encrypted. Entropy details in table 4 and figure (11, 12, 13, and 14).The samples entropy is maximized by using the key-generator with AES in medical images (table 4) will led to improve the security of the algorithm, the texture of the images are disappear in the encrypted images.

Table 4: Entropy

Image name	Entropy
Original sample 1	3.45114385987626
Encrypted sample 1	9.02627923737164
Original sample 2	8.39809460272765
Encrypted sample2	9.03615015385716

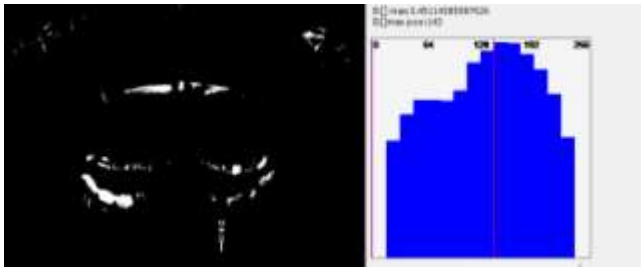

Figure 11: original sample 1 entropy

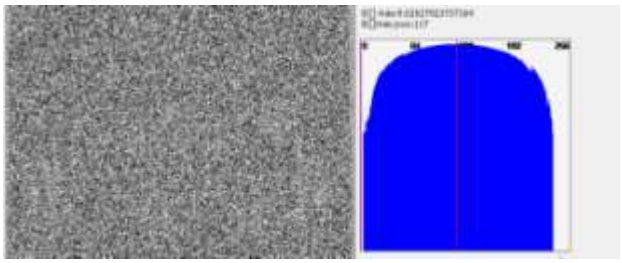

Figure 12: encrypted sample 1 entropy

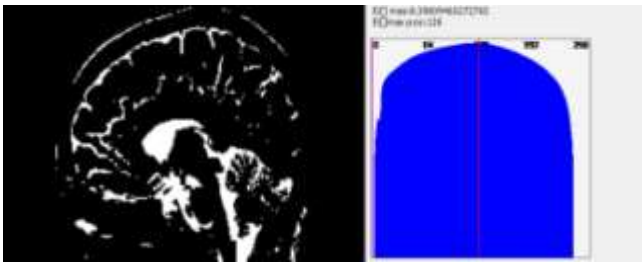

Figure 13: original sample 2 entropy

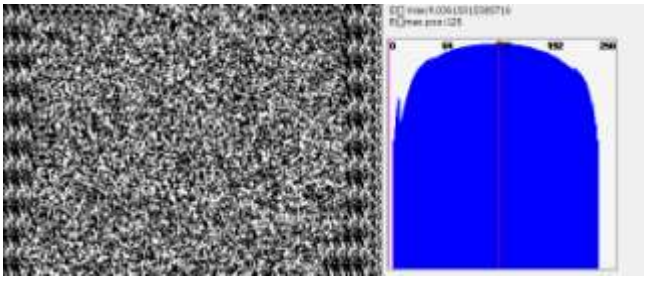

Figure 14: encrypted sample 2 entropy

The histogram details for all images are calculated, figure (15, 16, 17 and 18).

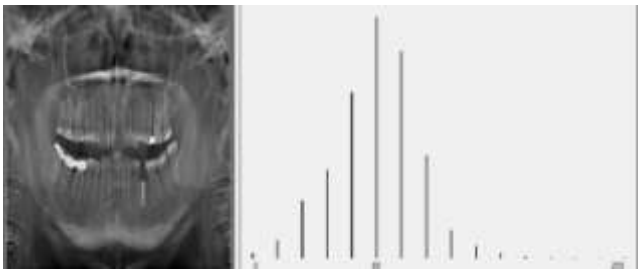

Figure 15: original sample1 histogram

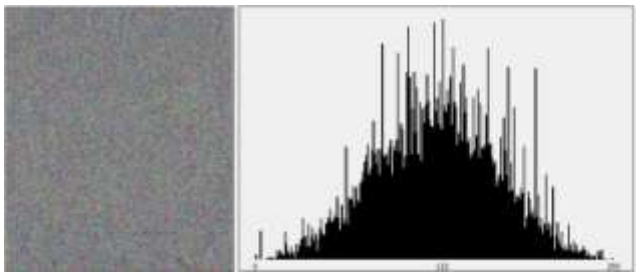

Figure 16: encrypted sample1 histogram

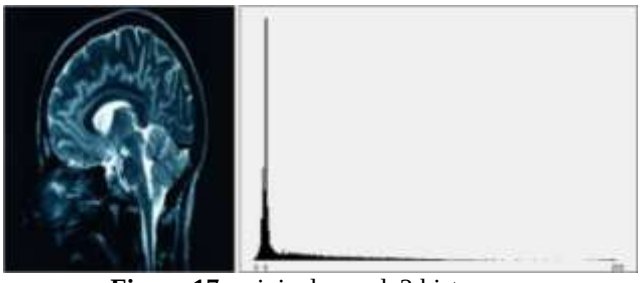

Figure 17: original sample2 histogram

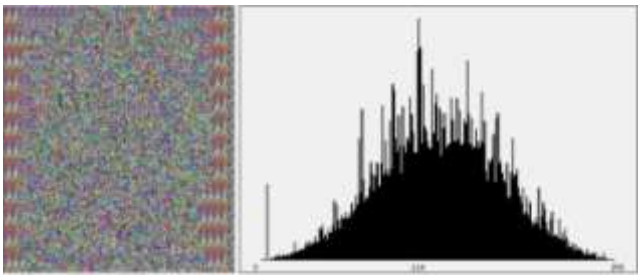

Figure 18: encrypted sample2 histogram

4.Conclusion

Modified AES algorithm is suggested, the symmetric encryption algorithm AES can be used for medical image encryption the proposed system extend the key scheduling and add A5/1 key generator to the system, which provide

more security and randomness to the encrypted data samples images, the version used for A5/1 algorithm that overcome the original algorithm problem and improve algorithm performance.

References

[1] Stallings, William, and Lawrie Brown. "Computer security." Principles and Practice (2008).
[2] Amutha, V., and CT Vijay Nagaraj. "A Secured Joint Encrypted Watermarking In Medical Image Using Block Cipher Algorithm." International Journal Of Innovative Research In Science, Engineering And Technology 3.
[3] Mohanad Ali, Hala Bahjat," Improvement Majority Function in A5/1 stream cipher Algorithm" Engineering & Technology Journal, Year: 2016 Volume: 34 Issue: 1 Part (B) Scientific Pages: 16-25.
[4] Biryukov, Alex. "Block Ciphers and Stream Ciphers: The State of the Art." IACR Cryptology ePrint Archive 2004 (2004): 94.
[5] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.
[6] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays", in: CT-RSA 2001, pp.84-99.
[7] J.J. Amador, R. W. Green "Symmetric-Key Block Cipher for Image and Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188