A Secure Framework For Medical Image Encryption Using Enhanced AES Algorithm

Manjula G, Mohan H S

Abstract: In recent years, with the enhancement of the progressive and innovative methods that is being used in day today activities, digital communication network has paved the way in the field of telemedicine for diagnosing diseases in secluded regions. Also with the adoption of cloud computing methods in the healthcare segment by most of the health care providers ,medical image data are now stored distantly in third party servers. Privacy, safety and security should be assured for such digital data by implementing encryption so as to ensure confidentiality and authentication methods to guarantee authorship. Henceforth the broadcasting of digital medical images over network has become common. Owing to deficiency of safety intensities on digital communication medium, digital medical image is constantly being vulnerable to attackers and other sources of security breaches. Due to these shortcomings it is quite complex to ensure security, integrity and robustness for digital medical image ad has become an significant concern. This forces for a necessity of robust and secure mechanism to broadcast the medical images over the Internet. To implement this we need to apply various security measures like cryptography and watermarking to the conveyed medical images so as to provide and protect the confidentiality of patient information. For using cryptography we need to utilize a more secure and robust process that will be undefeated for an extensive interval against dissimilar attacks. This proposed paper is based on using enhanced AES algorithm to encrypt patient data and hide it medical images and transmit it over communication medium. In this paper, we briefly evaluate the overall organization of Rijndael AES algorithm and a new dynamic S-Box is spawned using a Hash function to provide robust security.

Index Terms: Advanced Encryption standard (AES), Dynamic S-box, Performance analysis, Hash function, Cryptography, Security, Embedding

1. INTRODUCTION

In the present modern digital realm, providing authorized and protected access to the digital medical images which is warehoused on digital media is of paramount significance. The images warehoused on these digital media may be of varying size and large in number with most confidential data stored in them. Telemedicine is one such modern medical care application which facilitates the amalgamation of different communication and information structures into the field of healthcare structure. In the health care sector medical imaging has dominated major part of Health care Infrastructure. Remote diagnosis and consultation with reputed physicians ,accessing important medical archives, remote distance learning in the field of telemedicine are some of tremendous paybacks given for the users [1,2]. Nevertheless with these kinds of benefits, there are still affiliated jeopardies for medical data which is being socializing in the open networks, and consequently being effortlessly available to the intruders [3,4]. Hence it is the need of the hour for the professionals associated in the medical field for expressing their crucial requirement for protected edifices and also to exchange medical images and vital information. Therefore, three significant objectives in this regard are as stated as follows: 1) to defend the confidentiality of a given patient‘s information. and 2) to minimize storage requirement to the possible extent. 3) to save the overhead cost on the required storage medium and upsurge the speed of broadcast, but without corrupting the quality of the images. For transmitting medical images on a network we use different storage medium such as DVD,CD ,hard disks which would make a suitable choice requiring minimal or zero error coding and control techniques. To materialize these objectives many new clusters of expertise have been proposed and have been developed. One of them talks about secure protection of confidential data through cryptography where encryption is used. [5], [6]. Decryption of data In this category, requires appropriate key. The next method makes use of the water marking technique where the secret data which has to be transmitted is embossed into multimedia file and is then communicated over a network. When using any of these methods it is better to integrate them with the compression phase so as to maximize processing speed. Currently, performing encryption and compression together is the new challenge to be faced. The proposed works in this paper demonstrate how encryption algorithms are used to provide security to medical images by using Advanced AES algorithm. The principal goal is to achieve unbiased protection of medical images during transit. Whenever a patient visits a physician he may require to take second opinion regarding diagnosis and treatment. One probable solution to save time is to broadcast images which contains information of the patient together with a detailed report of the concerned specialist on the digital network. Nevertheless, the greatest potential risk encountered will be the complexity of the communication networks and the problems of security breaches. Hence we will be challenged with an actual security problem while conveying data on a digital transmission medium.

For ethical reasons, we cannot afford to transmit such important images over internet and it should be more secured. It can been highly recommended to use Encryption as a best solution for a situation like this. There has been many analysis to use various techniques for the encryption of text. When such encrypted medical image has to be sent over insecure channel we need to take of the quality of the image without noise affecting it. On the contrary, the arrival of sophisticated and modern computer expertise, and its infusion into the Medicine arena through E-health [7], Telemedicine [8-11], to tag a few, the scope and experiments of providing trusted confidentiality that derives from the concept of storage and communication of digital medical information is impossible to be handled by the physicians solely. Keeping all this constraints we can secure the medical images by using encryption algorithms.

- *Manjula G is currently pursuing her PhD from Visvesvaraya Technological University, Belgavi, Karnataka, India. E-mail: manjulayash1@gmail.com*
- *Dr.Mohan H S is currently working as Prof and Head, Dept. of ISE, SJBIT, Bangalore, India. E-mail: mohan_kit@yahoo.com*

2 RELATED WORK

Regardless of the growing solicitations in the area of telemedicine, and the instant prerequisite for ensuring much needed security services for telemedicine applications, research activity in this regard is gaining its importance. Different algorithms have been proposed widespread in this regard and have been suitably characterized depending upon the requirements.

2.1 Water Marking Techniques

Based on the content to be watermarked there exists mainly three different kinds of watermarking approaches which can been recommended watermarking medical images namely : a) irreversible methods, b) reversible methods and c) region-based methods [12-13]. In the first method i,e Irreversible watermarking methods the process involves distortion of image quality due to non-invertible operations like bit replacement, quantization ,truncation and so on [14-15]. On the contrary, it has been proved that Reversible watermarking methods permit the medical images to be reinstated to its original pixel values. This further ensures to make use of original medical images for necessary diagnosis. [16-20]. Even though it can be shown that most of the reversible water marking algorithms or approaches do not exhibit the quality of tamper localization which is very necessary for the verification of the integrity of medical data. The last method, region-based methods as the name suggests encompasses on dividing the original medical image into two distinct extents: region-of-interest (ROI) and region-of-non-interest (RONI).

.

2.2 Cryptographic Based Approach

Various modern cryptographic methods like symmetric ciphers, hashing methods and digital signature are being used to achieve security in the field of telemedicine and healthcare information systems.[21–24]. To address the security related issues in telemedicine a combined methodology utilizing the benefits of the two approaches, like water marking and crypto based algorithms have been addressed in various literature reviews. [25–28].

2.3 Hybrid Algorithm

In other approach a combination of watermarking and cryptographic primitives like CRC, hash code, MAC and digital signatures methods can be used to achieve security. In this approach watermarking can be used as the implementation platform and the authorized water marks which contain secret data can be encrypted using cryptographic approaches. The required security service can be embedded in the form of encrypted watermarks which are robust and fragile in nature.

3 CRYPTOGRAPHIC FUNCTIONS

Among modern cryptographic techniques, the Advanced Encryption Standard which is also identified as the Rijndael cipher algorithm [29],was designed by two Belgian research cryptographers Vincent Rijmen and Joan Daemen and after rigorous testing by the US organization National Institute of Standard and Technology (NIST), it was designated as the Advanced Encryption Standard (AES) Algorithm [30]. Rijndael AES cipher is accessible in US government publication, as FIPS-197 [31]. Advanced Encryption standard embraces of three block ciphers namely AES-28,AES-192 and AES-256.So ,each cipher in AES encrypts and decrypts data in terms of blocks each comprising of 128 bits of data making use of cryptographic key rings with sizes of 128,192 and 256 bits respectively. Since AES is an example which works on the concept of symmetric key algorithm it makes use of the identical key for both encrypting and decrypting the data and this makes the fact that mutually the communicating parties should communicate with the shared secret key beforehand in order to have secure transmission of data. Exclusively each and every round of both encryption and decryption operation have to clear through well- demarcated number of rounds defined as Nr rounds where Nr = 10,12,14 depending on the number of key size [33]. Figure 1 epitomizes the overall organization of standard AES.

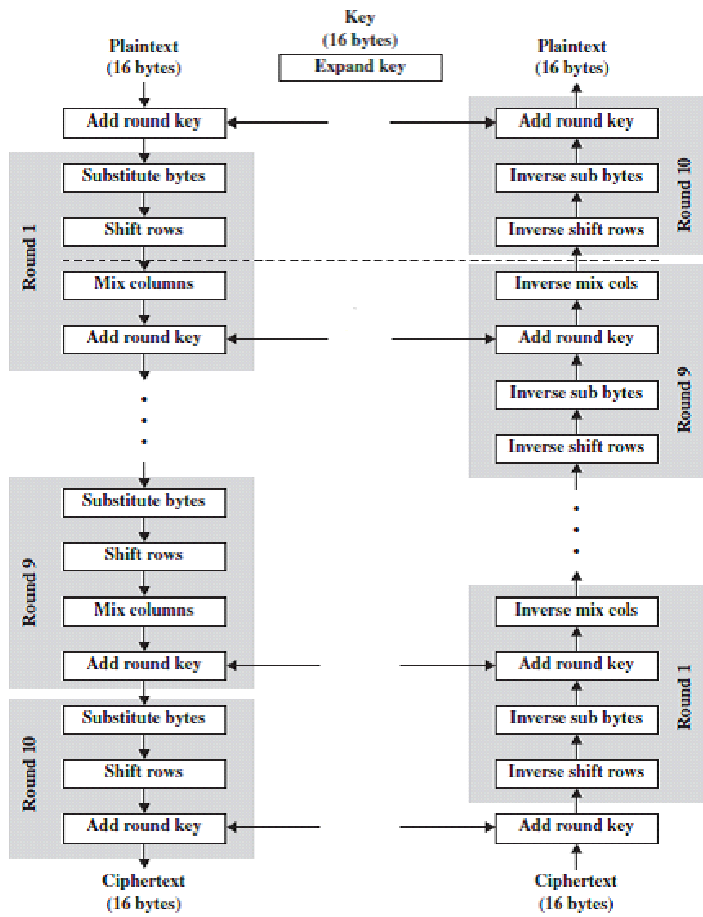


***Fig. 1**. AES algorithm*

The four transformations defined in each round of AES cipher are the following:

1. The ByteSub transformation: This is the initial task that has to be accomplished in every round in a nonlinear way on each of the State bytes independently. This is executed by using a standard pre-defined structure known as S- Box which is invertible.

2. The ShiftRow transformation: In this operation, each of the four rows of the state array is shifted to the left and the rows of the State array are episodically moved above diverse offsets.

3. The MixColumn transformation: In this transformation, each column of four bytes is converted by making use of a distinct mathematical function. Four bytes of input are accepted to this process and four entirely new bytes are produced which is further used for substitution of the original column bytes.

4. The Round Key addition: In this operation, 128 bit Round Key is EXORed with the 16 bytes of state array elements. The Round Key used for this purpose is acquired from the 128 bit Cipher Key by means of the key schedule process.

At the completion, the tenth round excludes the MixColumns operation.

4 PROPOSED APPROACH

Our framework for secure access to medical images is based on using advanced AES algorithm. The proposed methodology uses Hash function for designing Dynamic S- Box generation. The strength of the AES algorithm lies in S-Box design and they constitute the principal part of the encryption system.

4.1 Hash Function

In this segment the importance of using Hash functions in cryptography and how this is used in designing and generating a new S-Box is discussed. Hash functions are exceptionally beneficial and are implemented practically in all applications where information security is very critical. A Hash function can be described as an mathematical operation which accepts a numerical value of any length and always output a fixed length numerical value.

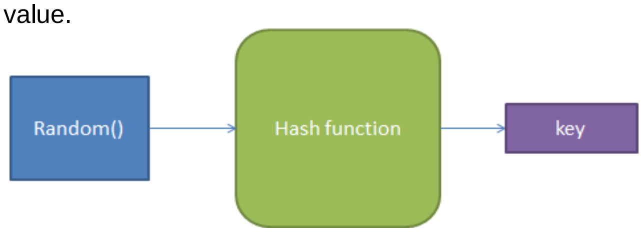


***Fig.2**. Initial Key generation using Hash Function.*

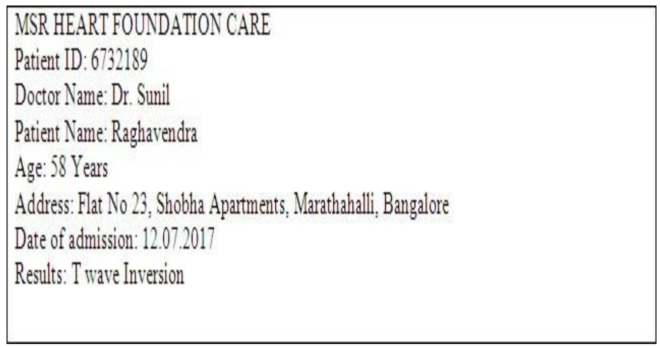
Message digests or hash values are the output produced by Hash functions. The input to the Hash function is selected by a random number generator and the output from the hash function is then utilized as the secret key to generate the new S-Box. The below Figure 3 depicts the way of generating of initial key [33].

The message digest generated from the hash function is then used to generate the new dynamic S-Box. The output created by the algorithm i.e the hash code length is important in contradiction to brute force attacks and this defines the strong suit of the hash code:

1. Pre Image resistance: For any given specified code h, it should be ascertained to be computationally impractical to derive x such that H(x) = h. To put in other way this property states that it is really very difficult to reverse a hash function.
2. Second Pre-Image Resistance: In case of any assured block x, it is computationally impractical to find y= x with H(y) = H(x). In a simplified way this characteristic feature states that for a given input value and its output hash, it would be tough to discover a different input with the same hash.
3. Strong collision resistance: It is to be proved computationally unfeasible to discover any such pair (x,y) such that H(x)=H(y) .In other words this characteristic property assures that it should be difficult to discover two different inputs of any length that result in the same result.

4.2 Generation of New S-box

The predefined static Standard S- Box used in AES algorithm has always an arrangement of 256 values of 8 bit numbers from 0 to 255 and this fact is utilized in the creation of the new S-Box .In the proposed methodology the use of the Hash function is mainly done to generate Dynamic S-Boxes. This process is created by using the following steps:


MSR HEART FOUNDATION CARE
Patient ID: 6732189
Doctor Name: Dr. Sunil
Patient Name: Raghavendra
Age: 58 Years
Address: Flat No 23, Shobha Apartments, Marathahalli, Bangalore
Date of admission: 12.07.2017
Results: T wave Inversion

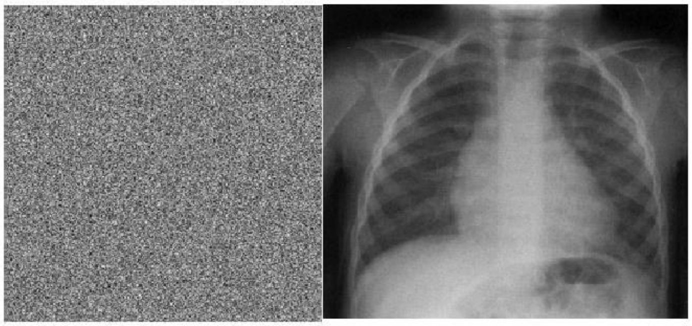
i. The output of the Hash function i.e. the input key is initialized as follows

```
for i=0 to 255
Key[i] = hash (random(x))
J=0;
for i=0 to 255
k[i]= key[i mod keylength];
J=(j+s[i]+k[i])mod 256;
exchange (S[i],S[j])
```

ii. The output of the above code produces 256 dissimilar values and this new set of created permutation values surely depend on the input key. If we change any one of the input key value, it generates another set of 256 different values.

iii. After generating 256 new set of values we should apply the affine transformation again to avoid any static facts of the S-Box and to make the box invertible since it is used in decryption.

5 EXPERIMENTAL RESULTS AND DISCUSSION



a) Original image b) Encrypted Image

***Fig.3**. Image encryption using AES 128 bit key.*

The following figure 4(a) and 4(b) demonstrates the original text and the encrypted test using the enhanced AES algorithm with new S-box generated.

a) Original Text

B89654CDE234BADE34519802F5432ACD45EDBDE189076FCA234789DCEF1234
AB54390CCDE2345ABC567EEFFDC2345679AC5410987678FFEDCAB54327801F
CDE36781290AFFEBBCDE12389ACE457BAE23FCE457781006543ABDEC2456FE
ADB3456FFEE456901AAC2345FEACB35678910FFE345ACEEFF345678654ACEFE
ADCB234568FE468EACB36577989ACCEFFB6543268AACEFF453645384758FFEA
B33765F5458943E654746BAEF5486748FE5478437ABC5874FF65384736EAB5648
5647FE735834890AAB4567FFE547FEAB6584675CE6965795FBAE68947590EF564
3CD6757

a) Encrypted Text

***Fig.4**. Using AES with 128 bit key to encrypt text.*

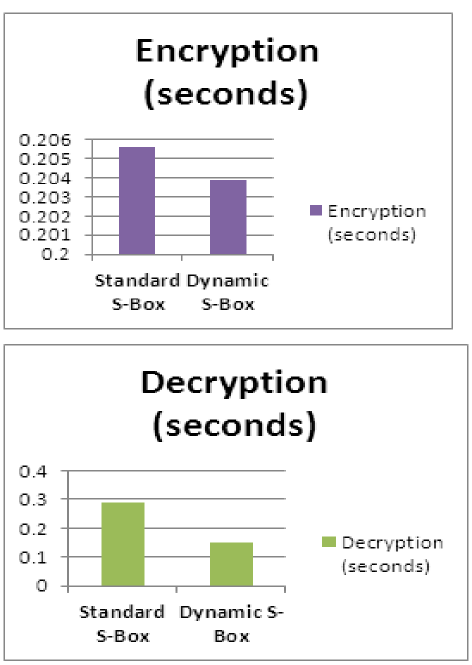


***Fig.5**. Encryption and Decryption Time*

6 CONCLUSION

As the speed of the network increases, security techniques becomes very complex. Henceforth very intelligent and secure encryption techniques should be used to transmit information via medical images. Embedding vital information of the patient and doctor must be transmitted without degrading the eminence of the cover image. Decoding the data at the receiver side is also very important and the processing time is also very important. The proposed security framework attempts to attain enhanced performance by dropping the encryption processing time and enhancing the quality of the stego image.

ACKNOWLEDGMENT

This research is supported by Visvesvaraya Technological University Jnana Sangama, Belagavi -590018 for grant of financial assistance.

REFERENCES

[1] Craig, J., Patterson, V. Introduction to the practice of telemedicine', J. Telemed. Telecare, 2005, 11, pp. 3–9
[2] Raghupathi, W., Tan, J.:Strategic IT applications in health care', Commun. ACM, 2002, 45, (12), pp. 56–61
[3] Ashley, R.: ‗Telemedicine: legal, ethical and liability considerations', J. Am. Diet. Assoc., 2002, 102, (2), pp. 267–269B.
[4] McEvoy, F., Svalastoga, E.:Security of patient and study data associated with DICOM images when transferred using compact disc media', J. Digit. Imaging, 2009, 22, (1), pp. 65–70
[5] B. Schneier. Applied cryptography. Wiley, New-York, USA, 1995
[6] A. Uhl and A. Pommer. Image and Video Encryption: From Digital Rights Management to Secured Personal Communication. Springer, 2005.
[7] National E-Health Transition Authority: About Us. National E-Health Transition Authority. 2013. Retrieved 2013-23-09.
[8] Padate, R., & Patel, A. (2014). Encryption and decryption of text using AES algorithm. International Journal of Emerging Technology and Advanced Engineering, 4(5), 54-9.
[9] Saylor, Michael (2012). The Mobile Wave: How Mobile Intelligence Will Change Everything. Perseus Books/Vanguard Press. p. 153.
[10] Conde, Jose G.; De, Suvranu; Hall, Richard W.; Johansen, Edward; Meglan, Dwight; Peng, Grace C. Y. (January/February 2010). "Telehealth Innovations in Health Education and Training". Telemedicine and e-Health 16 (1). p. 103-106. doi:10.1089/tmj.2009.0152.
[11] Coatrieux, G., Lecornu, L., Sankur, B., Roux, Ch.: 'A review of image watermarking applications in healthcare'. Proc. of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, New York, USA, 2006, pp. 4691–4694
[12] Coatrieux, G., Maitre, H., Sankur, B.: 'Strict integrity control of biomedical images'. Proc. of SPIE Security Watermarking Multimedia Contents III, SPIE 2001, San Jose, CA, January 2001, vol. 4314, pp. 229–240
[13] Berent, A. (2013). Advanced Encryption Standard by Example. Document available at URL http://www.networkdls.com/Articles/AESbyExample. pdf (April 1 2007) Accessed: June.
[14] Giakoumaki, A., Pavlopoulos, S., Koutsouris, D.: 'Secure and efficient health data management through multiple

watermarking on medical images', Med. Biol. Eng. Comput., 2006, 44, (8), pp. 619–631
[15] Thodi, D., Rodríguez, J.: 'Expansion embedding techniques for reversible watermarking', IEEE Trans. Image Process., 2007, 16, (3), pp. 721–730
[16] Celik, M., Sharma, G., Tekalp, M., Saber, E.: 'Lossless generalized-LSB data embedding',IEEE Trans. Image Process., 2005, 14, (2), pp. 253–266
[17] Celik, M.U., Sharma, G., Tekalp, A.M.: 'Lossless watermarking for image authentication: a new framework and an implementation', IEEE Trans. Image Process., 2006, 15, (4), pp. 1042– 1049
[18] Liew, S., Zain, J.: 'Tamper localization and lossless recovery watermarking scheme', Commun. Comput. Inf. Sci., 2011, 179, (1), pp. 555–566
[19] M. Aikawa, and K. Takaragi, Eds,J.1998. A Lightweight Encryption Method Suitable for Copyright Protection,In proceedings of IEEE Transactions on Consumer Electronics, Vol. 44, pp. 902–910.
[20] Guo, X., Zhuang, T.: 'Lossless watermarking for verifying the integrity of medical images with tamper localization', J. Digit. Imaging, 2009, 22, (6), pp. 620–628
[21] Mohamed, A. A., & Madian, A. H. (2010, December). A Modified Rijndael Algorithm and it's Implementation using FPGA. In Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on (pp. 335-338).
[22] Kobhayashi L.Furuie S:"Proposal for DICOM multiframe medical image integrity and authenticity "J. Digit Imaging 2011 24,pp 114-125.
[23] Bernarding, J., Thiel, A., Grzesik, A.: 'A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption', Int. J. Med. Inf., 2001, 64, pp. 429–438
[24] Acharya, U.R., Bhat, P.S., Kumar, S., Min, L.C.: 'Transmission and storage of medical images with patient information', Comput. Biol. Med., 2003, 33, pp. 303–210
[25] Shiguo, L., Zhongxuan, L., Zhen, R., Haila, W.: 'Commutative encryption and watermarking in video compression', IEEE Trans. Circuits Syst. Video Technol., 2007, 17, (6), pp. 774–778
[26] Puech, W., Rodrigues, J.M.: 'A new crypto-watermarking method for medical images safe transfer'. Proc. of 12th European Signal Processing Conf., Vienna, Austria, September 2004, pp. 1481–1484
[27] Zhou, X.Q., Huang, H.K., Lou, S.L.: 'Authenticity and integrity of digital mammography images', IEEE Trans. Med. Imaging, 2001, 20, (8), pp. 784–791
[28] Jain, R., Jejurkar, R., Chopade, S., Vaidya, S., & Sanap, M. (2014). AES Algorithm Using 512 Bit Key Implementation for Secure Communication. International journal of innovative Research in Computer and Communication Engineering NIST, ―National Institute of Standard and Technology,‖ http://csrc.nist.gov.
[29] J. Daemen and V. Rijmen, The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin, Germany / Heidelberg, Germany / London, UK / etc.: Springer-Verlag, 2002.
[30] Federal Information Processing Standards Publication (FIPS 197), ―Advanced Encryption Standard (AES),‖ 2001, http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf.
[31] A. Aziz and N. Ikram, ―Memory Efficient Implementation of AES S-boxes on FPGA,‖ Journal of Circuits, Systems and Computers (JCSC), vol. 16, no. 4, pp. 689– 694, August 2007.
[32] X. Yi, C. Tan, C. Siew, and S. Rahman,J.2001. Fast encryption for multimedia,In proceedings of IEEE Transactions on Consumer Electronics, Vol. 47, No. 1, page(s): 101 – 107.
[33] Manjula G, Mohan H S. "Improved Dynamic S-Box generation using Hash function for AES and its Performance Analysis", 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), 2018