Comparative Study on AES and RSA Algorithm for Medical images

Santhosh Kumar B J, Roshni Raj V K and Anjali Nair

***Abstract*—Scalability of network with the expanding number of system a data exchange is crucial to permit secure information transmission in the network environment. The sending information or image may defiled by any outsider on the off chance that it is not secured. In medical field it is essential to secure the data or images. There are many techniques available to ensure the security of images in medical field like RSA, AES, and Watermarking. RSA is a public key cryptographic technique, makes use of pair of keys (public key, private key) and AES is a private key cryptosystem and is based on Substitution Permutation Network. Using these techniques the host can encrypt and decrypt the image and can keep digital images safe. Watermarking is the process of hiding the information in any multimedia for the authentication and confidentiality of data. This paper recommends which is the best method among various techniques by considering every one of the techniques. By contrasting the different systems this paper can arrive at a conclusion that which is the best methods to guarantee the security of image.**

***Index Terms*—AES, Networking, Private Key, Public Key**

I. Introduction

A Personal computer (PC) system or a collection of systems are the medium which permits PCs to exchange data. Networking is the collection of systems connected each other to perform a specific task. The systems are connected through various cables like optical fiber, twisted pair cables etc. To define the architecture of any network many topologies are available such as ring, star, and bus etc. In a computer network framework, sender and receiver are the two parties to exchange the data. The protocols used to transmit the data over a network are TCP/IP, Ethernet, HTTP, SMTP, FTP, etc. There are two types of networking, connection oriented and connectionless where the connection oriented networking establishes a connection before sending the data, in connectionless networking there is no need of a connection.

Cryptography is an area which provide several policies to achieve privacy of the image includes confidentiality, authentication, security, integrity. It is necessary to protect the data which is transferring through internet or any medium. The data may attacked by third party .To ensure the integrity we have several techniques like RSA, AES. The proposed method compare these two techniques. Modem, router, gateway these are the hardware devices used to connect the computers in a network. The users cannot ensure its integrity while exchanging the data through a medium. The third individual may steal the image, edit the image quality or they can devastate it. In medical field, the Integrity of an image is significant. If they edit or destroy the image then it will affect the patient and as well as consultant. The rest of this paper is mentioned below. The literature review is described in Section II. Section III describes the existing system. The proposed work is described in Section IV. Section V says about the methodology. The simulation result is analyzed in Section VI. At last, Section VII concludes the paper.

II. Literature Review

"M. D. Amruth et al[1] this paper addresses the AES encryption algorithm for 512 bits.In this paper the Authors describing the features of AES in the cloud computing framewrok.The authors tries to proposing a new technique to provide more security in cloud computing".

"P. K. Rahul et al[2] this paper propose a hybrid technique. This paper is the combination of AES and NCC Cryptographic techniques. This paper provide good security by maintaining the key".

"R. Bhaskar et al[3] This paper addressing homomorphic Encryption for vector decomposition problem. Many techniques are available the authors provide a strong method to solve vector decomposition problem".

"A. R. Ganesh et al[4] provide a standard method to provide security and authentication by using two poplar technique like RSA and AES. To improve the calculation speed this paper used a technique called Vedic mathematics"

"Rahul et al[5] this paper is the analyst of the security threats in the hadoop technology framework. This paper uses the techniques like RSA, AES, and Hashing.RSA and AES is

Santhosh Kumar B J is with the department of computer science Amrita School of Arts and Sciences, Mysuru Campus, Amrita Vishwa Vidyapeetham, Amrita University, (Assistant professor)India
(email: santhoshbj50@gmail.com)
Roshni Raj V K is with the department of computer science Amrita School of Arts and Sciences, Mysuru Campus, Amrita Vishwa Vidyapeetham, Amrita University, India
(email: roshniraj2828@gmail.com)
Anjali Nair is with the department of computer science Amrita School of Arts and Sciences, Mysuru Campus, Amrita Vishwa Vidyapeetham, Amrita University, India
(email: anjalinair345@gmail.com)

978-1-5090-3800-8/17/$31.00 ©2017 IEEE

used for generating public key and private keys."

"Madhumita Panda et al[6] This paper comparing both private key (AES) and public key (RSA) cryptographic algorithms .It accepts varying types of input files like text, binary and image files. The parameters for these encryption algorithms are encryption time, decryption time and throughput".

"Manish Gupta et al[7] In the work they addressed new approach to protect the contents using image watermarking, asymmetric encryption and dictionary based compression hides target image within the cover image using image watermarking (LSB) and apply RSA algorithm for protecting watermarked image and then applies dictionary based compression for watermarked images. In this paper generating an image key from the encrypted watermarked image which increases the security. We also did compression to reduce the data to transfer in network to decrease the data load on network, it make fast transfer of information".

"Anil Kumar et al[8] The proposed method uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This method ensure that the message has been encrypted before hiding it into a cover image".

"V.Amutha, C.T. et al[9] This system based on approach which consolidates a substitutive watermarking algorithm with an encryption algorithm, advanced encryption standard (AES) in counter mode. AES used for encrypting the given transmission of data and medical image. Then digital watermarking technique used for encrypted data was hidden in the transmitted medical image".

"Ishwarya.V et al[10] In the proposed method is to provide authentication hash value will be created utilizing SHA and the Huffman compression algorithm(R-S vector) will be will be used to compress the size of an image. With the patient data the medicinal image is ensured through Public key cryptography in a secure manner. The quality measures such as PSNR, SNR, MSE and BER estimates the security of algorithms. This paper results the BER equals 0, SNR and SNR has a high consistent values. MSE have a low bit rate for all grayscale and color images".

"Mayuri Verma et al[11] This paper deals with the method of nesting digital images using watermarking, which makes use of an image inside another image and watermark is embedded into the main image which is the cover image. Here the LSB hiding algorithm is used for hide multiple images, The Blowfish algorithm is used to encrypt the watermark image before inserting into the cover image, because it will give more security for watermark image".

"Prerna Parmar et al[12] In this paper, we have proposed an algorithm for image security comprising watermarking in spatial domain along with encryption. At the resource, secret image which is a hidden image, is encoded in to a second image. This is done to cover image by watermarking, a pixel merging technique. Blowfish encryption is used for second method, the watermarked image encryption. The hidden image is finally decrypted by the receiving end of the tool".

"Abhilasha Sharma et al[13] In this paper mainly described watermarking methods based on transform domain techniques, that are discrete wavelet transform and discrete cosine transform .Here the embedding process, the cover watermark image is separated into two parts such us region of interest and non-region of interest. For authentication purpose here embedding multiple watermarks in the form of image and text on to the cover image. For enhancing the security ERP data encrypted by using RSA.Results shows that the proposed method is robust against various signal processing attacks and finally given high quality watermarked image".

"Vani Shaji et al[14] This paper talks about the accessible medical image watermarking strategies for protecting and authenticating medicinal information. As a lossless technique, the original image can be perfectly recovered by performing the reversible watermarking technique".

"CH.Venu Gopal Reddy et al[15] In this paper a double safety method of watermarking and encryption is recommended with a Multi-objective task for medical image watermarking to confirm that the watermark preserves its structural integrity with strength and imperceptibility".

"Shashi Mehrotra Seth et al[16] This paper has done the comparison of three algorithms such as DES, AES and RSA. The result was evaluated by certain parameters like memory usages, output byte and computation time, because the algorithms take a large amount of computing resources such as CPU time, memory and battery power and computation time".

"Sujata Nagpal et al [17] this paper proposed three technique i.e., Discrete Wavelet Transform, Neural Network and RSA encryption for image watermarking. The execution of the proposed plan is assessed on the premise of PSNR, MSE, NCC, BER and BCR. These parameters are utilized for checking the nature of the watermarked picture. Different attacks are applied on the watermarked image to check the robustness".

"Er. Pinki Tanwar et al[18] The watermarking can be set in host images or the host images can be encrypted with watermark without set explicitly in the host image. In this paper used three methodology DWT, RDWT, SVD and show the improvement of PSNR compare with existing system".

III. EXISTING SYSTEM

In modern times, all the data are present in a digitalized fashion. Individuals send information over wireless medium, or the internet. One can question the security and integrity of such data. For example ,images may be corrupted by a third-party and this may result in the loss of personal data .In an attempt to solve the above issues this paper provides certain techniques. Most of the existing papers discuss water marking technique or steganography to hide confidential images or sensitive data.

Drawback of watermarking technique is it gives negative impression among the users, because watermarked images are shown in the middle of main images and it will destroy the

perfection of the main image. Most of earlier work is based on either making use of conventional encryption and common public key cryptosystem. This application makes compares results of conventional encryption and public key systems.

IV. Proposed System

By considering different attacks on medical images by intruders, this paper suggests a few techniques which gives integrity to the image. The objectives of this paper is to compare two techniques (RSA, AES) which is used for encryption. By comparing these two methods the system will provide a more efficient in authentication and confidentiality. This paper comparing two techniques by calculating the buffer size of images. Compile time is the parameter used to measure the efficiency of images.

V. Methodology

A. RSA(Rivest-Shamir-Adleman)

RSA is a public key cryptographic technique to protect data from attacks. RSA can be used for encryption, key exchange (private and public key), digital signature.RSA is designed by Ron Rivest, Adi Shamir, and Leonards in 1978. In RSA any person can encrypt the data but for decryption it can be only done by the authenticated receiver. This encryption rely on cryptographic algorithm. In this framework, application is proposed to encode and decode the brain images by makes use of RSA algorithm, makes use of two keys, d (private key) and e(public key), both work in pairs, for encryption and decryption, respectively. The original image P is encrypted to encrypted image C by

C = Pe mod n

The encrypted image is retrieved by

P = Cd mod n

Because of symmetry in modular arithmetic, encryption and decryption are mutual reverses and commutative. Therefore,

P = Cd mod n = (Pe) d mod n = (Pd) e mod n

B. AES (Advanced Encryption Standard)

AES based on Substitution Permutation Network. Using these techniques the host can encrypt and decrypt the image and they can keep their digital images safe. AES encompasses three block ciphers, AES-128, AES-192 and AES-256. All cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Secret-key ciphers use the same key for encoding and decoding the images, so both the sender and the receiver must know and use the same secret key.

A) *Comparison*

In this paper two cryptographic techniques are comparing to calculate efficiency. The comparison is done by calculating the buffer size. Finally this comparison finds which algorithm is more efficient by considering the given set of data.

VI. Results

These are the graphs which shows the result of comparison of RSA and AES in compile time.

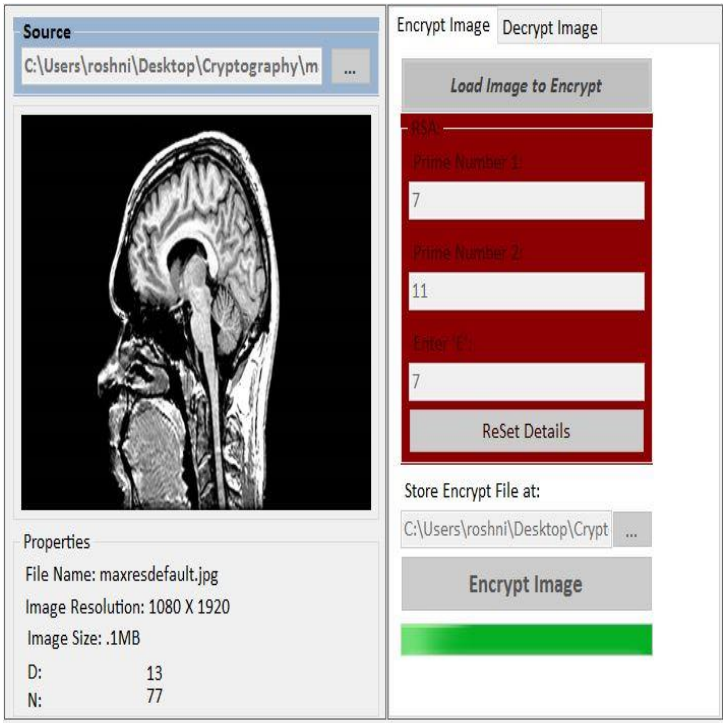

Fig. 1. Encryption of brain images

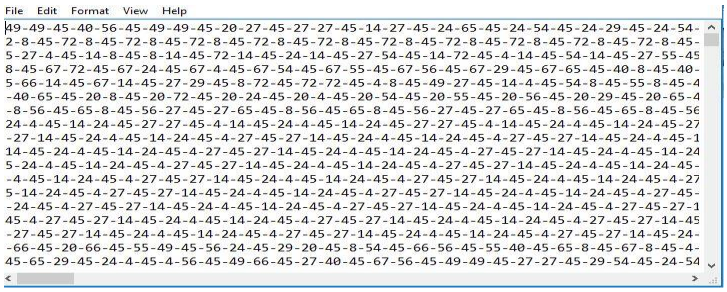

Fig. 2. Encrypted result

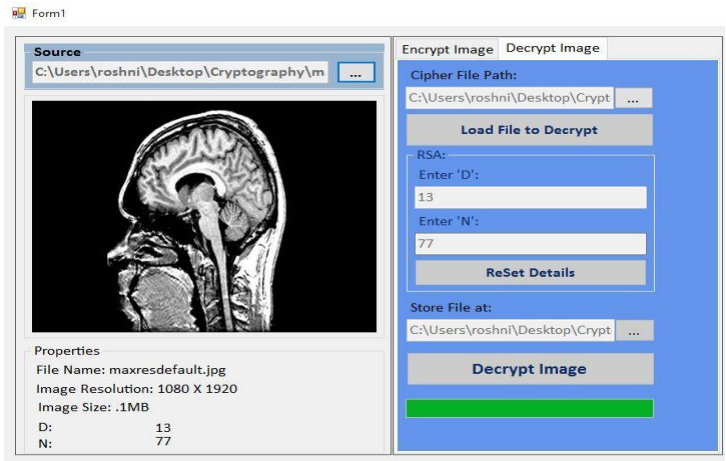

Fig. 3. Decryption of brain images

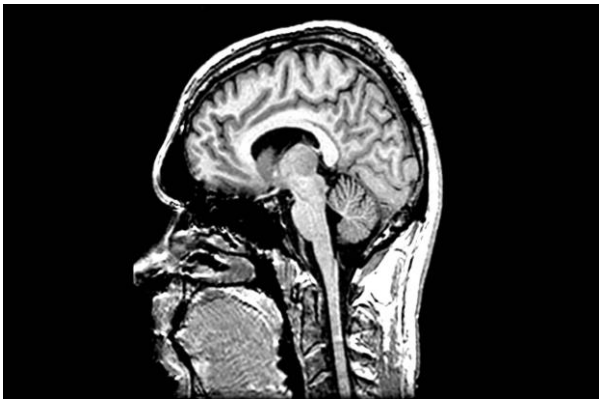

Fig. 4. Decrypted result

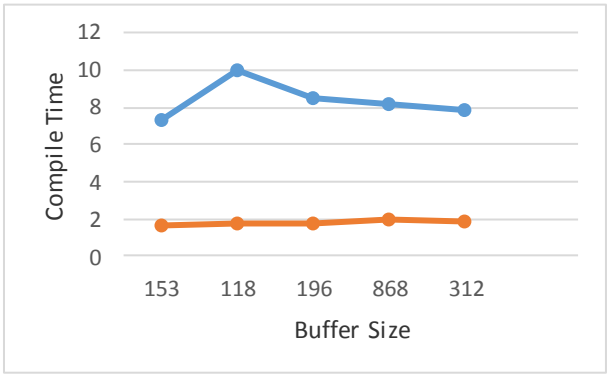

Fig. 5. Chart shows Encryption compile time of RSA and AES

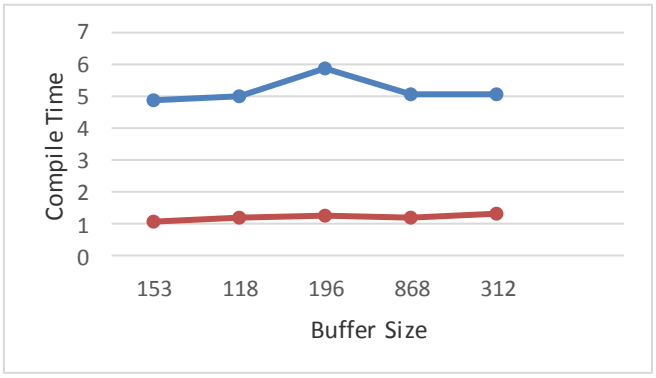

Fig. 5. Chart shows Decryption compile time of RSA and AES

CONCLUSION

This Paper addresses the comparison of two popular cryptographic techniques (AES and RSA).The comparison is done by calculating the buffer size of images. By comparing these techniques the paper come to a conclusion that AES is more efficient in both encryption and decryption, for the given set of data.

REFERENCES

[1] M. D. Amruth and Praveen, K., "Android smudge attack prevention techniques", Advances in Intelligent Systems and Computing, vol. 385, pp. 23-31, 2016.[Abstract]

[2] P. K. Rahul and Gireesh, K. T., "A Novel Authentication Framework for Hadoop", in Artificial Intelligence and Evolutionary Algorithms in Engineering Systems: Proceedings of ICAEES 2014, Volume 1, P. L. Suresh, Dash, S. Subhransu, and Panigrahi, K. Bijaya New Delhi: Springer India, 2015, pp. 333–340.

[3] R. Bhaskar, Hegde, G., and Vaya, P. R., "An efficient hardware model for RSA encryption system using Vedic mathematics", in Procedia Engineering, Coimbatore, 2012, vol. 30, pp. 124-128.

[4] A. R. Ganesh, Manikandan, P. N., Sethu, S. P., Sundararajan, R., and Pargunarajan, K., "An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks", in International Conference on Recent Trends in Information Technology, ICRTIT 2011, Chennai, 2011, pp. 1209-1214.

[5] S. T., S., K., and V., S. K., "Enhancement of cloud security using AES 512 bits", Research Journal of Applied Sciences, Engineering and Technology, vol. 8, pp. 2116-2120, 2014.

[6] M. Panda, "Performance Analysis of Encryption Algorithms for Security," 2016.

[7] M. Gupta, R. Gupta, G. Parmar, and D. Anand, "A New Approach for Information Security using Asymmetric Encryption and Watermarking Technique," vol. 57, no. 14, pp. 1–5, 2012.

[8] Kumar and R. Sharma, "International Journal of Advanced Research in A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," vol. 3, no. 7, pp. 363–372, 2013.

[9] V. Amutha and C. T. V. Nagaraj, "A Secured Joint Encrypted Watermarking In Medical Image Using Block Cipher Algorithm," vol. 3, no. 3, pp. 1099–1104, 2014.

[10] V. Ishwarya, "Secure Sharing of Medical Information in Watermarked Image through Telemedicine using PKI Technique," vol. 101, no. 2, pp. 14–18, 2014.

[11] M. Verma and S. Verma, "LSB Hiding Using Random Approach For Image Watermarking," pp. 2319–2321, 2014.

[12] P. Parmar and N. Jindal, "Image Security with Integrated Watermarking and Encryption 1 1 2," vol. 9, no. 3, pp. 24–29, 2014.

[13] Sharma, A. K. Singh, and S. P. Ghrera, "Secure Hybrid Robust Watermarking Technique for Medical Images," vol. 70, pp. 778–784, 2015.

[14] V. Shaji and V. V Prakash, "Securing Medical Images Using Digital Watermarking," pp. 140–145, 2015.

[15] H. Venu, G. Reddy, and P. Siddaiah, "International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) A Dual Security Approach for Medical Images using Encryption and Watermarking Optimized by Differential Evolution Algorithm," pp. 17–29, 2015.

[16] S. M. Seth and R. Mishra, "Comparative Analysis of Encryption AlgorithmsFor Data Communication," vol. 4333, pp. 292–294, 2011.

[17] M. M. Abd-eldayem, "original article A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," Egypt. Informatics J., vol. 14, no. 1, pp. 1–13, 2013.

[18] E. P. Tanwar and E. M. Khurana, "International Journal of Advanced Research in Improved PSNR and NC in Digital Image Watermarking Using RDWT and SVD," vol. 6, no. 5, pp. 955–959, 2016.

[19] J. S. Bhalla and P. Nagrath, "Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm," vol. 3, no. 4, pp. 1–6, 2013.

[20] J. M. Education, C. Science, S. Nagpal, S. Bhushan, and M. Mahajan, "An Enhanced Digital Image Watermarking Scheme for Medical Images using Neural Network , DWT and RSA," no. April, pp. 46–56, 2016.