ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

An Advanced Crypto Based Security System for Medical Image/Data Transfer

Aparna K S[1], Sreejith R[2], Ambikadevi Amma T[3]

M.Tech Student, Department of CSE, Jawaharlal College of Engineering and Technology, Lakkidi, Kerala, India [1]

Assistant Professor, Department of CSE, Jawaharlal College of Engineering and Technology, Lakkidi, Kerala, India [2]

Professor and Head, Department of CSE, Jawaharlal College of Engineering and Technology, Lakkidi, Kerala, India [3]

ABSTRACT: The protection of data is of at most importance in the medical field to boost the telemedicine applications. There is a need of robust and secure mechanism to transfer the medical images over the Internet. This system proposes a method for protecting medical images. It is capable of providing basic security services such as confidentiality, authenticity and integrity to medical images exchanged in various applications with a tamper localization scheme. Here makes use of a crypto based algorithm based on strong cryptographic functions with internally generated symmetric keys and hash codes. The advanced encryption standard-Galois counter mode authenticated encryption function is primarily used in implementation providing confidentiality and authenticity with the whirlpool hash function and elliptic curve digital signature algorithm is used to provide integrity. The proposed algorithm is based on the digital imaging and communication in medicine (DICOM) standard with the enhancement in its security functionalities. In this system incorporated a tamper localization scheme by using Least Significant Bit (LSB) based Watermarking without dividing image into blocks.

KEYWORDS:Medical imaging, Security, DICOM standard, AES-GCM, WSH, ECDSA, Watermarking, Tampering

I. INTRODUCTION

The necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the network. In number of medical applications, special safety and confidentiality is required for medical images. Therefor security is increasingly playing a relevant role in the healthcare field in order to provide services like information integrity, authenticity and confidentiality. The Digital Imaging and Communications in Medicine (DICOM) standard is the worldwide accepted standard for medical images, and it addresses security issues in its Part 15 [2]. However, there is still room for improvement in the approach proposed in DICOM in order to enhance image integrity and authenticity. Many works in this field rely on the use of watermarking, but this approach has issues that may limit its use in the medical field. The crypto-based approach for achieving security in the medical information exchange systems is based on the application of cryptographic functions such as symmetric encryption, hashing and digital signatures. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message is called symmetric encryption. It provides confidentiality for the transmitted images using block ciphers and stream ciphers. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. It is used in many encryption algorithms. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. In this work Implementing a crypto-based algorithms capable of providing confidentiality and verifying authenticity and integrity of DICOM images with tamper localization scheme. Unlike the DICOM standard and other crypto-based schemes, the proposed algorithms provide confidentiality, authenticity and integrity for both constitutes of the DICOM images: the header data and the pixel data. Strong cryptographic functions with externally and internally generated symmetric keys and hash codes are used in the implementation of the algorithms. A major contribution of the algorithm is the strong bond

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

established between the pixel data and header data and also included a tamper localization with the application of reversible watermarking scheme without any division of medical images.

Tamper localization is necessary when deals with Medical images because it can locate where the alteration of the image is. In this system incorporated a tamper localization scheme by using Least Significant Bit (LSB) based Watermarking without dividing image into blocks. This allows content-based integrity rather than the strict-integrity functionality implemented by the current algorithms for avoiding unnecessary retransmission of DICOM images. Aim of this work is to solve the security limitations of DICOM images for its secure transmission through network for various healthcare application

Paper is organized as follows. Section IIdescribe the related work, Methodology is given in Section III. Section IV presents experimental results showing results of image tested. Finally, Section V presents conclusion.

II. RELATED WORK

Recently, the introduction of information technology in the medical field has boosted the evolution of various healthcare applications. Medical Image Sharing is a term for the electronic exchange of medical images between hospitals, physicians and patients[1]. Cryptography enables to store sensitive information or transmit it across insecure networks like the Internet so that it cannot be read by anyone except the intended recipient. DICOM stands for Digital Imaging and Communications in Medicine and it is the most universal and fundamental standard in digital medical imaging [2,3,11]. it provides all the necessary tools for the diagnostically accurate representation and processing of medical imaging data. DICOM is not just an image or file format but It is an all-encompassing data transfer, storage, and display protocol built and designed to cover all functional aspects of digital medical imaging.[4]

The algorithms in medical image field can be classified into three watermarking- based algorithms, crypto-based algorithms and hybrid algorithms. Watermarking and Hybrid methods involves segmentation of the original medical images, this prevent it from possible future adoption by medical security standards and professionals. The crypto based algorithms provide confidentiality, integrity and authenticity for the header and pixel data of DICOM images through the use of three effective cryptographic functions. The three functions are the advanced encryption standard-Galois counter mode (AES-GCM), the whirlpool hash function and the elliptic curve digital signature algorithm.

The Advanced Encryption Standard (AES) is a symmetric block cipher algorithm. This algorithm allows for a variety of block and key sizes and not just the 64 and 56 bits as of DES' block and key size. The block and key can be chosen from 128, 160, 192, 224, 256 bits and need not be the same. No of rounds depends on size of the key chosen.[[11,17,18]. AES-GCM is an authenticated encryption function which is primarily used in applications demanding confidentiality, authenticity and integrity. it offers symmetric encryption and authentication at the same time. GCM or the Galois Counter Mode is a mode of operation for the AES block cipher that provides Authenticated Encryption [5,7,14]. Authenticated Encryption is a mode of a block cipher encryption which provides not just confidentiality but integrity/authenticity too.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Elliptic Curve Digital Signature Algorithm or ECDSA is a cryptographic algorithm uses elliptic curve cryptography (ECC) to produce shorter signatures than the original DSA. A hashing algorithm is a cryptographic algorithm that can be used to provide data integrity and authentication [6,9].Whirlpool is a block-cipher-based secure hash function. It produces a hash code of 512 bits for an input message of maximum length less than 2256 bits. We can use the whirlpool hash function in security applications because of the fact that no attacks have been reported on earlier versions of the function.

The ability of tamper detection in medical images is essential for authentication. There are many methods and algorithms for tamper localization in medical image processing such as using fragile watermarks, feature based approach, embedding cryptographic signature and block identifier, using deformable templates etc[15,16]. But all of them divides medical image into blocks and each block is embedded with the authentication message and recovery information of other blocks. Dividing medical images may leads to fault diagnosis so these techniques are not suitable

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

for medical images [19,20].Tamper localization without dividing significant part images are more suitable in case of medical images

III. PROPOSED METHODOLOGY

In this system a cryptographic mechanism of advanced encryption standard-Galois counter mode, Whirlpool hash function and Elliptic curve digital signature algorithm is used for assuring the integrity, security and confidentiality level. This methodology is runs in two levels. Those are Encryption and signature generation and Decryption and signature verification.

A. Basic algorithm

Extract the header data and pixel data from a DICOM file and then uses symmetric encryption, hashing and digital signatures to provide confidentiality, integrity and authenticity for the header and pixel data of DICOM images.

Pixel data Encryption and Decryption

Extract Header and pixel data from DICOM file. Pixel data is image data. Then divide image in to Region of Interest(ROI) and Region of Non Interest(RONI). Fix ROI as square. Then extract data from ROI and then calculate hash value of that extracted data using whirlpool secure hash function. Embed this hash code as watermark in RONI using reversible watermarking, the LSB replacement technique. Details of Division of image is encoding in DICOM file that is to be sent. The watermarked image is encrypted using AES-GCM algorithm. Symmetric key and initialization vectors used for encryption are produced from hash code of header data. Hash code of Header is also encrypted using AES algorithm and stores it in DICOM header for decryption as Shown in figure.1

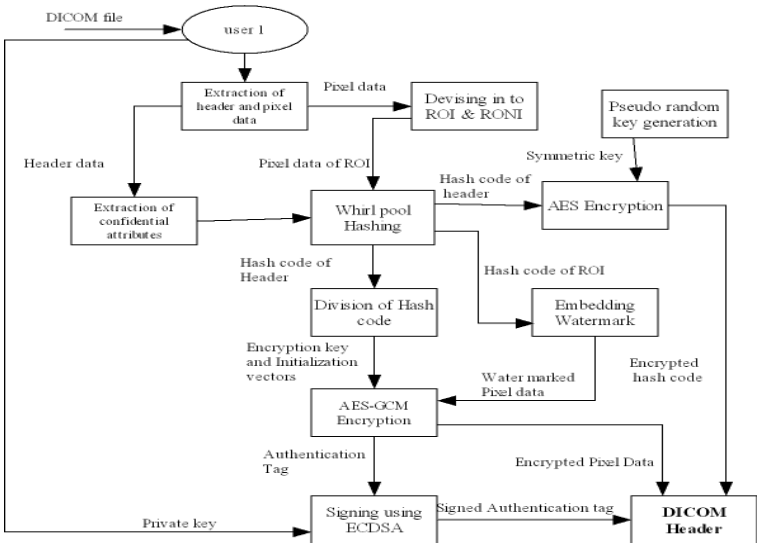


Figure1:Pixeldata encryption

User extract all Datas stored in Encrypted DICOM file for Decryption process. Encrypted Pixel data is Decrypted using AES-GCM, the Decryption key and Initialization vectors are produced from Decrypted hash code of header using AES algorithm. After Decryption we get two outputs Water marked pixel data and an authentication tag. For authentication verification procedure, Generate Authentication data from signed data using ECDSA, compare two values if they are equal image is not tampered else tampered. Divide Water marked image into ROI and RONI using information encoded in file. Remove water mark then we get original pixel data. If the image is tampered check whether tampering is on ROI. For tampering localization calculate hash of ROI from original pixel data and check whether it is equal to removed watermark, if they are equal image is Not tampered at ROI else Resend the file as shown in Figure. 2)

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

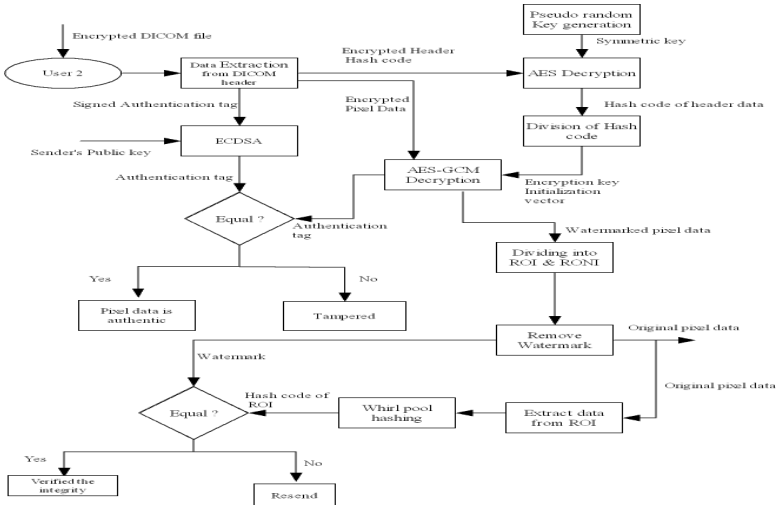


Figure2: Pixel data decryption and verification

Header Data Encryption and Decryption

This procedure reads all confidential attributes of the header data from DICOM file, then encrypts these datas using AES-GCM algorithm and stores the result in DICOM header. The encryption key and initialization vector used by AES-GCM to encrypt the header data are taken from the hash code pixel data produced by applying the whirlpool hash function on the pixel data. The hash code is then encrypted using AES algorithm and stored in the DICOM header for later use. Out puts of AES-GCM encryption are Encrypted header data and an authentication tag. Authentication tag is signed with the private key of the sending entity using ECDSA and stored in the DICOM header, shown in figure.3

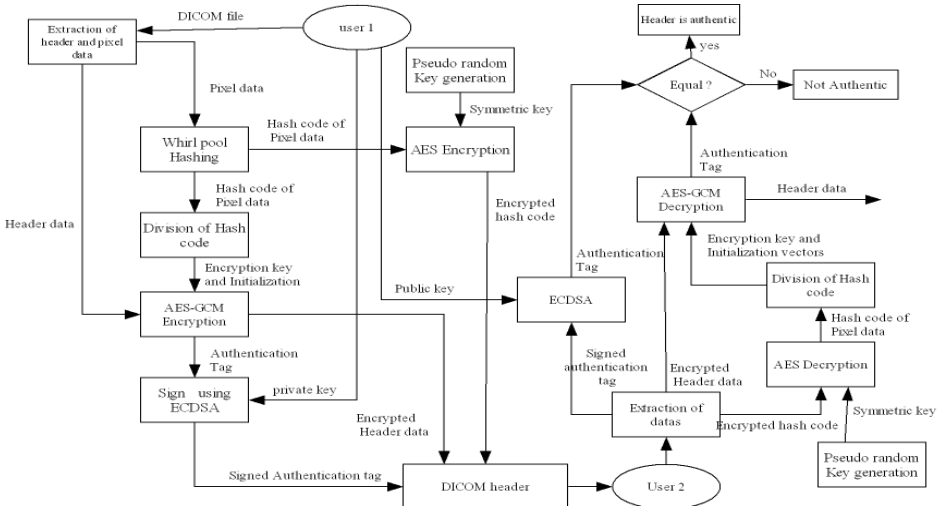


Figure 3:Header data encryption and decryption

Extract encrypted datas from DICOM file. Encrypted header data is decrypt using AES-GCM algorithm. Decryption key and Initialization vectors are Produced from Decrypted hash code of pixel data using AES algorithm. AES-GCM produces authentication tag and original header data. Retrieve the digital signature of the header data from the DICOM header and extract its authentication tag using the public key of the sending entity. Compare the extracted

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

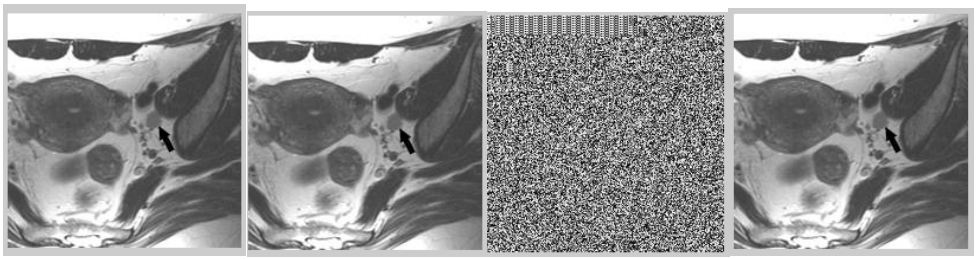
Vol. 5, Issue 6, June 2016

tag with the authentication tag generated by AES-GCE in the previous step. If a match exists between the two tags, authenticity and integrity of the header data is verified.

IV. EXPERIMENTAL RESULTS

Figures shows the results of Encryption and Decryption of Medical image using Crypto based algorithm with tamper localization scheme.The experiments wereconducted in a graphical user interface (GUI) based MATLABenvironment running on a Dell N5010 machine (Intel Core TM,4.00 GB RAM, and M 350 at 2.27 GHz with Microsoft Windows 7 operating system). Figure1 shows the constructed image from the extracted Pixel data from the DICOM file.Then next figure is watermarked image using simple LSB method then the image of encrypted image using AES-GCM algorithm also the next is decrypted image using the same algorithm.

Figs.(1) shows the original image. (2) Watermarked image.(3)Encrypted image. (4)Decrypted image



(1) (2) (3) (4)

V. CONCLUSION

Medical image transmission is the most important task in the real world which needs to be done for treating the patients in the efficient manner. Security is the most concerned issue that arises in the medical image transmission process. In this work secured transmission of DICOM medical images are done by introducing the cryptographic based encryption scheme. The proposed crypto-based algorithm is developed to provide confidentiality, authenticity and integrity for DICOM files exchanged between medical entities considering tamper localization scheme. Unlike the DICOM standard and other DICOM-based cryptographic algorithms, the proposed algorithm provides the required security services for the pixel data as well as for the header data. The algorithm is implemented using strong cryptographic primitives such as AES-GCM, the whirlpool hash function and the ECDSA and incorporates a tamper localisation scheme to allow for content-based integrity rather than the strict-integrity functionality implemented by the current algorithms. Tamper localization is a useful functionality because integrity control based on the exact preservation of all parts of the image may be unnecessarily strict as distortions on the image may also be due to noise originating from the transmission process .Generating the encryption key and initialization vector internally creates a strong link between the pixel data and header data. Different DICOM files have different data thus the encryption key and initialization vector vary from one image to another. This reduces security risks and avoids introducing a potential vulnerability in the encryption process.

REFERENCES

[1] 1. Luiz Octavio Massato Kobayashi, Sergio Shiguemi Furuie, and Paulo Sergio Licciardi Messeder Barreto, “Providing Integrity and Authenticity in DICOM Images”, IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 4, July 2009.

[2] Huijuan Yang and Alex C. Kot,” Binary Image Authentication with Tampering Localization by Embedding Cryptographic Signature and Block Identifier”, IEEE Signal Processing Letters, Vol. 13, No. 12, December 2006.

[3] Gouenou Coatrieux, Clara Le Guillou, Jean-Michel Cauvin, and Christian Roux, “Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images”, IEEE Transactions on Information Technology in Biomedicine, Vol. 13, No. 2, March 2009

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

[4] Hongjie He, Fan Chen, Heng-Ming Tai, Ton Kalker, and Jiashu Zhang, "Performance Analysis of a Block-Neighborhood-Based Self-Recovery Fragile Watermarking Scheme", IEEE Transactions on Information Forensics And Security, Vol. 7, No. 1, February 2012
[5] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux," A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 5, September 2012
[6] 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
[7] Siau-Chuin Liew & Siau-Way Liew & Jasni Mohd Zain, "Tamper Localization and Lossless Recovery Watermarking Scheme with ROI Segmentation and Multilevel Authentication", J Digit Imaging (2013) 26:316–325
[8] Osamah M. Al-Qershi and Bee Ee Khoo, "Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images ",Journal of Digital Imaging, Vol 24, No 1 (February), 2011: pp 114Y125
[9] Luiz O. M. Kobayashi, and Sergio S. Furuie, "Proposal for DICOM Multiframe Medical Image Integrity and Authenticity", Journal of Digital Imaging, Vol 22, No 1 (February), 2009: pp 71Y83
[10] Gueron, S.: „AES-GCM for efficient authenticated encryption – ending the reign of HMAC-SHA-1?". Workshop on Real-World Cryptography, Stanford University, USA, 2013
[11] Mariusz Dzwonkowski, Michal Papaj, and Roman Rykaczewski, "A New Quaternion-Based Encryption Method for DICOM Images", IEEE Transactions on Image Processing, Vol. 24, No. 11, November 2015
[12] Rouzbeh Maani, Sergio Camorlinga & Neil Arnason, "A Parallel Method to Improve Medical Image Transmission", J Digit Imaging (2012) 25:101–109
[13] Adina Arthur, Saravanan V, "Blackfin processor based secure medical image audio and video transmission technique for tele medicine considering online applications", Procedia Engineering, Volume 38, 2012, Pages 359–365
[14] Md shohidul Islam, Jongmyon Kim, Ui-pil Chong, "GPU based high speed error protection for watermarked medical image transmission", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:2, 2014
[15] Deo Brat Ojha, Ajay Sharma, Abhishek Dwivedi, Nitin Pandey, Amit Kumar, "An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel", Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 841-845 (2011)
[16] Sonika C. Rathi and Vandana S. Inamdar, "Medical Images Authentication through Watermarking Preserving Roi", Health Informatics - An International Journal (HIIJ) Vol.1, No.1, August 2012
[17] Gran badshag, Siau-Chuin Liew, Jasni Mohd Zain, Tutut Herawan, "Tamper localization and recovery medical image watermarking: A Review", International conference on computational science and information management, vol 1, PP:267-270, 2012
[18] Xiaotao Guo and Tian-ge Zhuang, "Lossless Watermarking for Verifying the Integrity of Medical Images with Tamper Localization", Journal of Digital Imaging, Vol 22, No 6 (December), 2009: pp 620Y628
[19] Mehri Owjimehr, Habibollah Danyali, "Medical Image Watermarking for Tamper Localization and Recovery of Region of Interest",
[20] Shu-Chien Huang, "An ROI-Based Medical Image Tamper Detection and Recovery Scheme"