Digital Signature Based on DICOM Standards of Medical Image by JAVA (DSMI)

Chun Jin, Ling-ling Zhou, and Xiao Wang

***Abstract*—In order to ensure the integrity of the patient information, undeniability, authenticity and reliability, the safety of telemedicine treatment and the regional PACS(Picture Archiving and Communication Systems) transmission, this paper designs digital signature of ECDSA(Elliptic Curve Digital Signature Algorithm)in DICOM(Digital imaging and Communications in Medicine)medical images during the rapid development of digital and information in telemedicine and medical care. we generate keys and digital certificates by OpenSSL toolkits, which can realize certificate management and generate keys. This paper also realizes digital signature by JAVA, which has advantages of Cross-platform, easy transplantation, high safety and so on .**

***Index Terms*—PACS, DICOM, ECDSA, digital signature**

I. Introduction

Medical field has close connection with human life, which follows step of area all the time such as the rapid development of electronic medical records, telemedicine and so on. Breakthrough of compute technology, especially network communication, high speed computing devices and image acquisition and processing of the software and hardware, provides digital technological base for digital acquisition, storage, management, processing, transmission and effective use of medical images. Digital medicine is perfect combination, which connects information technology and medicine. It also has been developed as a definite direction. During the rapid development of digital and information in telemedicine and medical care, hospital information system has been used more and more popular and also has been connected with other hospital's information system [1]. Security of medical information will become more important and prominent [2], because privacy data of patients gradually exposed to open environment.

During diagnosis and treatment, a series of health records and medical images are generated, stored, transmitted, and withdrawn, so the security of medical information research has become necessary[3].

In America, there is a representative principle, which is promoted by the U.S. government ,called Health Insurance Portability and Accountability Act(HIPAA) [4], [5]. In the HIPAA, privacy and security regulations are the two crucial parts that indicate how to avoid offenses and unauthorized disclosures of health information. Nowadays, the HIPAA is a popular framework that is followed by a great number of organizations. In our country, there are less researches in the part of privacy and security regulations, so we must make more effort in it. In Chapter 15 of the DICOM[6] (Digital Imaging and Communication in Medicine) Standard, it has security model of digital signature in DICOM files. In appendix C of DICOM standard, it has digital signature model of RSA [7], [8], but it didn't provide specific implementation of digital signature in DICOM files. This paper designs digital signature of ECDSA in DICOM medical images by JAVA. ECDSA（Elliptic Curve Digital Signature Algorithm） is the discrete logarithm problem which based on the point group of elliptic curves in finite fields . Compared to RSA, it has advantages of Small key size, saving bandwidth and storage space.

Manuscript received July 23, 2012; revised September 2, 2012. This work is supported by the Innovation Fund Project of China (Project ID: 11C26215113536) and science and technology key projects of Chongqing Science and Technology Commission (NO.CSTC2011AC2109, NO.CSTC2011AC2179).

Chun Jin is with Chongqing University of Posts and Telecommunication, Chongqing 400065,China.He is also with Chongqing JinOu Science and Technology Development Co .Ltd., Chongqing 400041, China (e-mail: jinchun@cqupt.edu.cn).

Ling-ling Zhou is with Chongqing University of Posts and Telecommunication, Chongqing 400065, China. (e-mail:zhouling198523@163.com).

Xiao Wang is with Chongqing Broadcasting and TV Group,4 00039,Chongqing,China.

II. Safety Regulations of Dicom Standard

In chapter 15 of DICOM standard, it has proposed security system structure model of digital signature in DICOM file which can satisfy some Characteristics such as data confidentiality, data authentication, data integrity, source key management. This model Contains the following information: the roles of the signer, signature property list, the mechanism of producing and validating the signature, and how to identify signer, and other relationship with digital signature, other factors which are used to create, calibration and explain the signature. In mechanism of producing and validating the signature, it also contains creating MAC or disorder yards of algorithm and related parameters (tag (0400,0015)), encryption algorithm and parameters, certificate type or release mechanism (tag (0400,0110)),etc .

III. Elliptic Curve Digital Signature Algorithme

A. Generation of ECDSA Signature

Know number: message m, global parameters (F_q, E, G, q, a, b, h) and key pairs (Q, d) ;Q of limited domain $a, b \in F_q$,based on F_q : $y^2 = x^3 + ax + b$; $q = p$ or based on F_{2^m} : $y^2 + xy = x^3 + ax^2 + b$, $q = 2^m$; E is elliptic

curve in F_q; G is one of rational points in E that is base point ,the order of G is n, $n > 2^{160}$, $n > 4\sqrt{q}$; h is a one-way security hash function .

1) Choosing a random number k, $k \in [1, n-1]$;
2) Calculating $kG = (x_1, y_1)$;
3) Calculating $r = x_1 \bmod n$;if $r = 0$, go back to step(1);
4) Calculating $k^{-1} \bmod n$;
5) Calculating $e = SHA1(m)$;
6) Calculating $s = k^{-1}(e + dr) \bmod n$,if $s = 0$,go back to step(1);
7) Signature of message is (r, s) ;

B. Validation Algorithm of ECDSA

Receiving message m and signature (r, s) ,global parameter $D = (q, F_q, a, b, G, n, h)$, public key Q .

1) Checking r , s , r , $s \in [1, n-1]$;
2) Calculating $e = SHA1(m)$;
3) Calculating $w = s^{-1} \bmod n$;
4) Calculating $u_1 = ew \bmod n$, $u_2 = rw \bmod n$;
5) Calculating $X = u_1 G + u_2 Q$;
6) $X = 0$, invalid signature; Otherwise, $X = (x_1, y_1)$,calculating $v = x_1 \bmod n$;
7) $v = r$,valid signature; Otherwise, invalid.

IV. Digital Signature Realiztion Process of Dicom Medical Images

A. Development Environment and Toolkits

Development language is JAVA, development platform is MyEclipse. Although it has integrated a lot of safety tools and the ability of cross-platform in JAVA, which can realize the authentication center, the support of certificates is not perfect. It can only support existing certificates, but it can not produce new certificates .This paper can achieve producing and issuing digital certificates by OpenSSL[9].

B. CA and Digital Certificates

The whole package of OpenSSL mainly can be divided into three main function parts: password algorithm library, SSL protocol library and application. In OpenSSL, CA application is a small certificates management center, which can issue the whole process of certificates and most of certificates management mechanism[10].This paper generates CA and issuing certificates by OpenSSL toolkits, and also gets private key and public key of signed certificate by JAVA. Because in JAVA, the format of private key is PKCS#8, we must convert private file to PKCS#8 by using pkcs8 command in OpenSSL, that is the key of getting private key.

C. DICOM Digital Signature Process

Digital signature scheme is a kind method of electronic form of storage news signature. A complete digital signature scheme should be made by the two parts: the signature algorithm and validated algorithms. Generally speaking, any public key cryptosystems can be used as a digital signature scheme separately .We can sign all tags by using elliptic curve encryption algorithm for digital signature of DICOM files and it can ensure the integrity of the information, but when the message is long ,the efficiency of signature is also low. This paper uses high-efficiency message-digest algorithm and elliptic curve encryption algorithm ,that is ECDSA.

The whole signature of DICOM medical images, as shown in Fig.1:

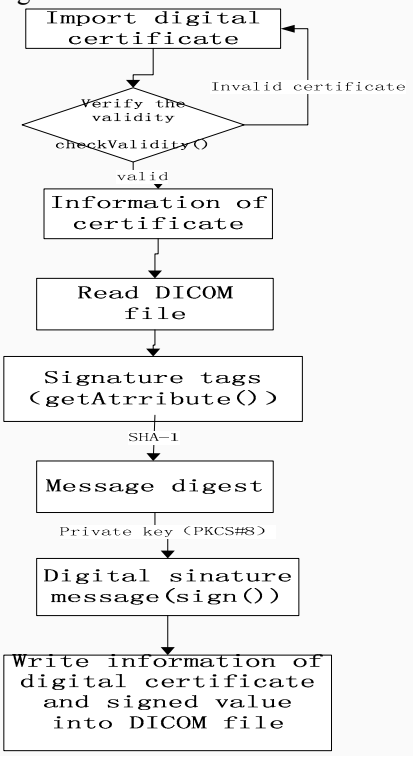

Fig. 1. Digital signature

1) Importing one of certificates from certificates library and then reading information of this certificate by using methods of CertificateFactory. getInstance("X.509"), FileInputStream() and generateCertificate().Verifying the effectiveness of the digital certificate by using method of checkValidity(),if it is true，getting information of certificate, such as version(getVersion()),serial number(getSerialNumber()), issuer(getIssuerDN()),sign algorithm(getSigAlgName()).
2) Reading a DICOM file,we can judge if it is or not a DICOM file by the method of getImageReadersByFormatName("dicom").DICOM files generally have two parts: DICOM file headers and data sets.
3) Choosing signature tags .According to DICOM images content levels,we choose parts of tags. There are four content levels in DICOM images: Patient, Study, Series, Image .Every level has a information entity that is Patient IE, Study IE, Series IE, Image IE. There are not specific signature tags in DICOM standard, this paper chooses some tags such as SOP Instance UID, Patient's Name, Patient ID.
4) Getting signature tags by the method of getAttributeString(Tag.PatientID) and so on, we can produce a length of 160 bit digest message by using

secure hash algorithm (SHA-1).

5) Reading the private key of PKCS# 8 format from the corresponding certificate. We sign the digest message by the private key. From this ,we produce signature.
6) Writing signature and information of certificate into Corresponding labels of DICOM file ,such as MAC Algorithm(0400,0015), Data Elements Signed(0400,0020), Certificate Type(0400,0110),Certificate of Signer(0400,0115).

V. Vertify Process of Dicom Images

Proof procedure ,as shown in Fig.2:

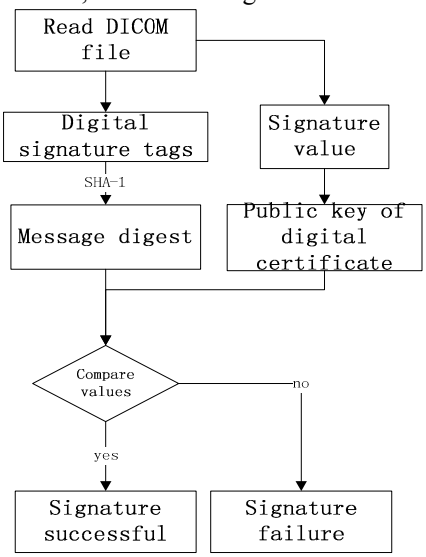

Fig. 2.Vertify process

1) Getting signed tags from Data Elements Signed (0400, 0020) tag of signature file. The tags are the same as tags during signed process.
2) Producing a length of 160 bit digest message(hashA) by using tags which getting from step 1 with secure hash algorithm (SHA-1).
3) Getting signed value of sender by reading the tag of Signature (0400, 0120).
4) Getting public key from digital certificate. Calculating with signed value by public key, then we can get hashB.
5) Comparing hashA with hashB. If it is true, signature successful, otherwise, failure.

VI. Conclusion

We realize digital signature of DICOM images based on ECDSA by study and research of DICOM standard. From the result of the experiment, ECDSA is available for medical images based on DICOM to signature and validation. We also produce CA and issue digital certificates by toolkit of OpenSSL.Fig.3 is issued digital certificate. Fig.4 is the information of certificate from MyEclipse.

Fig.5 is unsigned DICOM file tags. From Fig.5,we can see some tags such as (0400,0015), (0400,0020), (0400,0110), (0400,0115), their value is 00H. Fig.6, Fig.7, Fig.8, Fig.9 are signed parts of DICOM tags: MAC Algorithm(0400,0015),Data Elements Signed(0400,0020), Certificate Type(0400,0110),Certificate of Signer(0400,0115).

Fig. 3. Signed digital certificate

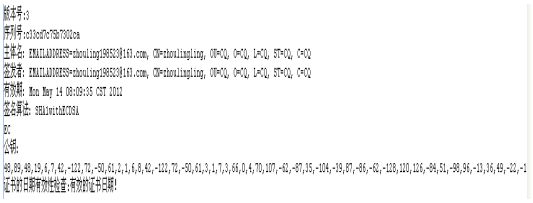

Fig. 4. Information of certificate from my eclipse

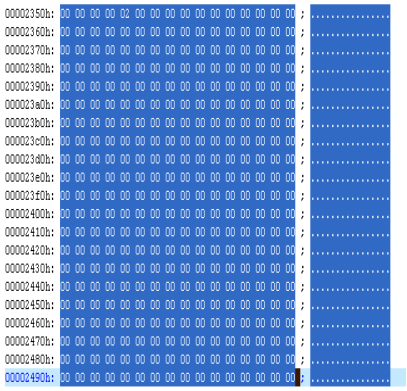

Fig. 5. Unsigned tags

Fig. 6. Tag (0400,0015)

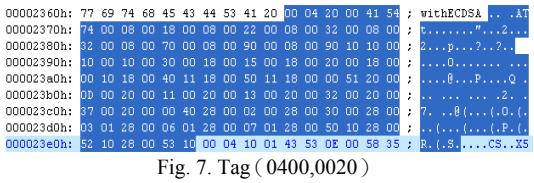

Fig. 7. Tag (0400,0020)

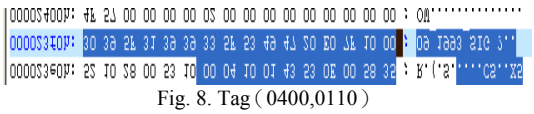

Fig. 8. Tag (0400,0110)

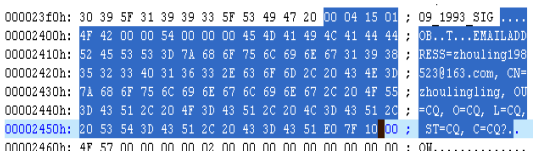

Fig. 9. Tag (0400,0115)

References

[1] X. Lv, L. Wang, and J. Zhao, "Research and Implementation of the TLS Network Transport Security Technology Based on DICOM Standard," *Inner Mongolia University of Science and Technology*, China, pp. 23-24, 2012.

[2] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring individuals' concerns about organizational practices," *MIS Q*, vol. 20, pp. 167–196, Jun. 1996.
[3] J. G. Hodge, L. O. Gostin, and P. D. Jacobson, "Legal issues concerning electronic health information: Privacy, quality, and liability," *J. Amer. Med. Assoc*, vol. 282, pp. 1466–1471, 1999.
[4] Health Insurance Portability and Accountability Act of 1996, 104th Congress, Public Law 104–191, 1996.
[5] Centers for Medicare nd Medicaid Services. (1996). *Health Insurance* Portability *Accountability Act of 1996 (HIPAA)*, [Online]. Available: http://www.cms.hhs.gov/hipaageninfo.
[6] HEMA. DICOM: Digital Imaging and Communication in Medicine. (Jan. 2011). [Online]. Available: http://medical.nema.org/
[7] X. Zhang, "Digital signature and technology," China: Chengdu, pp.108-128, 2004.
[8] Y. Zhang and A. Zhang, "Comparison of RSA and ECDSA in digital signature," *Southwest Jiaotong University*, Cheng Du, pp.96, 2010.
[9] Z. Wang, X. Tong, H. Shen, "Open SSL and Internet information security- foundation, structure and instruction," China: Beijing, 2007.
[10] H. Zhang, W. Zeng, and T. Jiang, "Authentication center by JAVA and Open SSL," China, pp.157-159, 2004.

Chun Jin was born in 1966. He is a doctor, Professor of Chongqing University and Chongqing University of Posts and Telecommunication ,general manager and the chairman of Chongqing JinOu Science&Technology Development Co.Ltd,. Mainly engaged in software engineering, wireless network technology, the embedded system, the vehicle communication system, and other aspects of the technology and product research and development, 9 published books, more than 50 published academic papers, obtained more than 40 patents, won two progress prize in science and technology.

Ling-ling Zhou was born in 1985. She is a graduate student. She is studying in Chongqing University of Posts and Telecommunication. Her current research area includes image processing, neural computation, distributed computing, wireless communication, medical images and information security.

Xiao Wang is a bachelor. He is chief engineer of Chongqing broadcasting group(station). His current research area include wireless communication, digital TV technology, HD news broadcast platform system