International Journal of Intelligent Information Systems
2018; 7(4): 38-41
http://www.sciencepublishinggroup.com/j/ijiis
doi: 10.11648/j.ijiis.20180704.11
ISSN: 2328-7675 (Print); ISSN: 2328-7683 (Online)

Medical Image Authentication Using Quartic Digital Signature Algorithm

Santhosh Babu, Viswanath Kapinaiah

Department of Telecommunication Engineering, Siddaganga Institute of Technology, Tumkur, India

Email address:
santhoshmehtre@gmail.com (S. Babu), kviitkgp@gmail.com (V. Kapinaiah)

To cite this article:
Santhosh Babu, Viswanath Kapinaiah. Medical Image Authentication Using Quartic Digital Signature Algorithm. *International Journal of Intelligent Information Systems.* Vol. 7, No. 4, 2018, pp. 38-41. doi: 10.11648/j.ijiis.20180704.11

Received: December 11, 2018; **Accepted**: January 15, 2019; **Published**: January 31, 2019

Abstract: The transmission of medical data in remote places using telemedicine technology requires secured and authenticated data transmission. In this paper, a novel technique is proposed to address authenticated mode of transmission using digital signature which incorporates curve coordinate system. The authentication functions and hash codes are used in the proposed algorithm and the keys are generated for secure transmission. The use of Quartic Digital Signature Algorithm (QDSA) provides authenticity and integrity. The Signature generated encapsulated in the DICOM header and transmitted to the receiver for verification. The proposed technique is demonstrated and evaluated using different modalities of DICOM images.

Keywords: DSA, Medical Image, DICOM, Devil's Curve

1. Introduction

Telemedicine is used to communicate patient and the doctors who are in remote places for diagnosis. The revolution of image analysis and inclusion of communication and information security plays a vital role in telemedicine applications. Exchange of medical data in the network which is prone to compromising the security of the medical data so there should be some special standards that deal with medical data security issues [1]. Digital Imaging Communication in Medicine (DICOM) standard provides a set of guidelines to achieve authenticity, confidentiality and integrity of the data. A DICOM file contains Header and image data in a single file. Header consists of constant and standard information [2].

Confidentiality protects data from third party entity that are not authorized to access the data. Authentication is the assurance such that the both the entity involves in the communication can claims each other. Integrity assures data from source is not modified, inserted or deleted by any other entity and received data exactly same. To provide security to the medical data crypto based security mechanisms are used. Encryption is the technique which provides confidentiality in exchanging the data in the network which is applied in telemedicine. Digital signature algorithms provides integrity and authentication of the records transmitted during telemedicine [3].

In this paper a curve based digital signature authentication scheme for medical images is proposed which authenticate the medical data. The existing digital signature schemes are Digital Signature Algorithms (DSA) and Digital signature based on elliptical curve cryptography [4].

2. Cryptographic Schemes

2.1. Integer Factorization

In integer factorization select p, q which is prime number and compute n where n=p*q. it is easy to calculate n if p and q is known, if n is known and it is feasible to calculate p and q for certain range but it is computationally infeasible to find p and q if both prime numbers are large. Security depends on the difficulty of factoring large values of p and q.[5]

2.2. Discrete Logarithmic

It is based on finite theory. If g & h Є G then gx =h, where G is acyclic group is called discrete logarithm to the base g of h in the group G.DSA, the curve based encryption systems are based on discrete logarithm. The difficulty in this algorithm is if the quantum computers are unknown by the algorithm then cryptosystem in infeasible.[5]

3. Existing Authentication Techniques

3.1. Digital Signature Algorithm

The authenticity of digital data can be obtained by mathematical model known as Digital Signature Standard. They provide a layer of validation as well as security to messages sent through a non-secure channel. DSA is based on computational difficulty in finding discrete logarithm. DSA consists of three parameters which are made public to some group of users. Digital signature Standard algorithm is as follows:

Global Public key:

Consider a prime number p and q prime divisor of (p-1) which depends on bit length L. Where

$p\ 2^{L-1} < p < 2^{L}$ &

$q\ 2^{159} < q < 2^{160}$ with L=160 bits.

$g=h^{(p-1)/q} \bmod p$, with 1<h< (p-1)

Private Key of sender:

Random or pseudorandom integer *x* with *0<x<q*

Public Key of sender:

$y=g^{x} \bmod p$

Secret number:

Secret number which is random or pseudorandom number k with *0<k<q*

Signature Generation:

$r= (g^{x} \bmod p) \bmod q$

$s=[k^{-}1(H(m)+xr)] \bmod q$

signature=(r, s)

Verification:

$W=(s`)^{-1} \bmod q$

$U_1=[H(m`)w] \bmod q$

$U_2=(r`)w \bmod q$

$V=[(g^{u1}y^{u2}) \bmod p] \bmod q$

3.2. Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic curve digital signature technique is implemented on elliptic curve, ECDSA has three phases, key generation, signature generation and signature verification.

ECDSA key generation:

Considering sender A's key which is associated with elliptical curve parameters. Each entity A follows these steps:

1. Select random integer'd' in interval [1 n-1] which private key.
2. Compute public key Q=dP, where P is a prime of order n.
3. A's public key is Q and A's private key is d.

ECDSA signature generation:

To sign a message m each entity A follows these steps:

1. Select a random integer 'k' in interval [1 n-1].
2. Compute kP = X1, Y1. And r=X1 mod n.if r = 0 go to step 1.
3. Compute k-1 mod n.
4. Now find s= k-1 {h(m)+dr} mod n. h= hash algorithm (SHA-1), if s=0 go to step 1.
5. (r, s) is the signature of m.

ECDSA signature verification:

Receiver B receives copy from sender A and follows these steps to verify the signature:

1. Signature (r, s) is integer or not in interval [1, n-1].
2. Calculate w =s-1 mod n and h(m)
3. Find u1=h(m)w mod n and u2=rw mod n
4. Compute u1P + u2Q = (X0, Y0), v= X0 mod n
5. If v=r then signature is verified.[6]

4. Proposed Algorithm

The random key generation in Digital Signature algorithm leads to poor authenticity. The curve coordinate based algorithm explained in this paper strengthen the selection of the random key which depends on the following parameters.i) a, b the real numbers ii) order of the curve iii) the prime value [7] Proposed algorithm consists of signature creation procedure and signature verification procedure. The description of these two procedures is as given in this section:

Quartic Digital Signature Algorithm:

A geometrical curve based novel technique is developed to provide authentication of the data. A curve defined in Cartesian coordinate plane with general equation $y^2\ (y^2-a^2) =x^2\ (x^2-b^2)$ this curve is called Devil's curve [8, 9]. From this general equation of devil's curve for a=0.8 and b=1 curve is as shown in Figure 1.

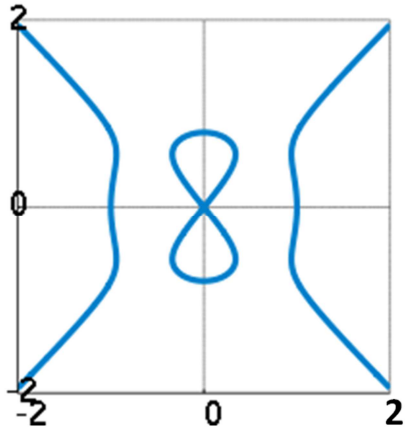

Figure 1. *Devils curve for a=0.8 and b=1.*

Images are expressed in different points, considering these points in algorithm to form different curves which helps in different applications like curve modification and fitting in image processing. The properties of Devil curve supports image processing techniques like curve fitting algorithm, pattern recognition and computer aided geometric design. This research implements a novel Digital Signature Algorithm technique for providing authentication on medical images based on Devil's curve concepts [10, 11].

Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. This section proposes a new variant of digital signature algorithm based on difficulty of solving x^{th} root problem.

The algorithm involves three phases.

1. Key generation.
2. Signature Generation.
3. Signature Verification.

The key generation and signature generation carried out in the sender's side. The received data along with the signature is verified by the signature sent by transmitter. If signature is invalid the receiver discards the data and transmits the indication such that the received data is not authenticated. Compare to conventional signature algorithm this paper describes curve based signature algorithm.

The flow chart of the proposed method shown in the Figures 2, 3, 4 respectively.

A) Key Generation

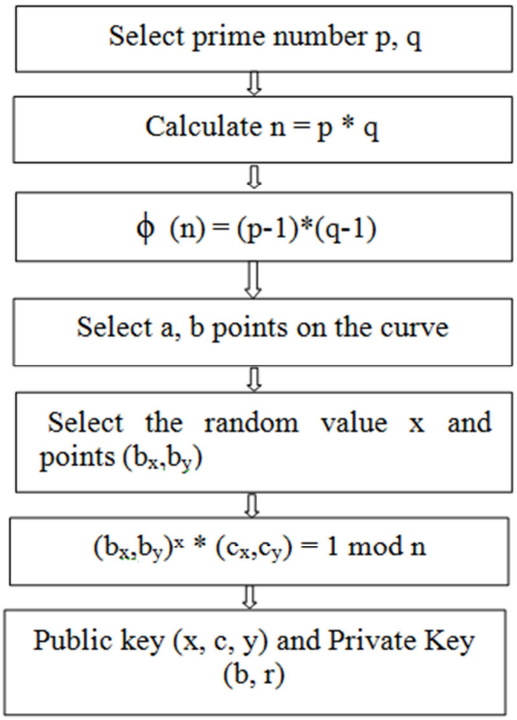

Figure 2. *Key Generation.*

B) Signature Generation

Transmitter Side

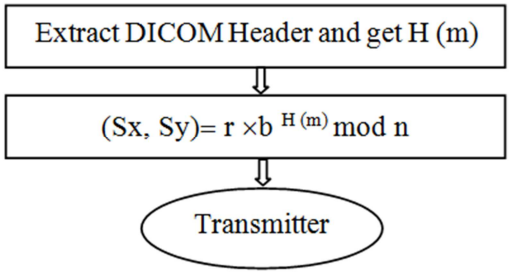

Figure 3. *Signature Generation.*

C) Signature Verification

Receiver Side

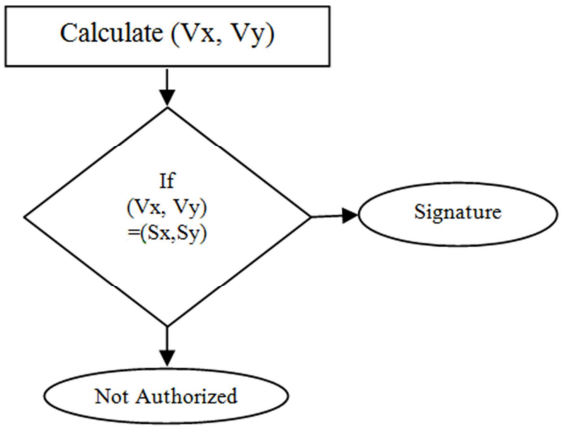

Figure 4. *Signature Verification.*

Proof of correctness of the algorithm:

LHS = $((s_x, sy)^x \times (c_x, CY)^{H(m)}) \bmod n$

$= (((r_x,r_y) \times (bx,by)^{H(m)})^x \times (c_x,c_y)^{H(m)}) \bmod n$

$=((r_x,r_y)^x \times ((bx,by)^x \times (c_x,c_y))^{H(m)}) \bmod n$

= y = RHS

5. Results

Consider the curve $y^4-4y^2-x^4+81x^2$ over prime field is $y^4-4y^2-x^4+81x^2=1 \bmod (n^2-n+41)$.

Where n =4, since it's a quartic curve. Degree is 4.

$n^2-n+41=4^2-4+41=53$ (According to Euler's theorem).

$y^4-4y^2-x^4+81x^2=1 \bmod 53$.

Where $a=2$ and $b=9$ are the real numbers.

Table 1. *Shows the generated points on the curves according to curve equation selected.*

x	13	40	5	48	6	47	25	28	2	17	7
y	4	4	7	7	8	8	11	11	15	15	3

Table 1. Points generated by the following curve $y^4-4y^2-x^4+81x^2=1 \bmod (n^2-n+41)$.

Graph generated by the selected polynomial is shown in Figure 5.

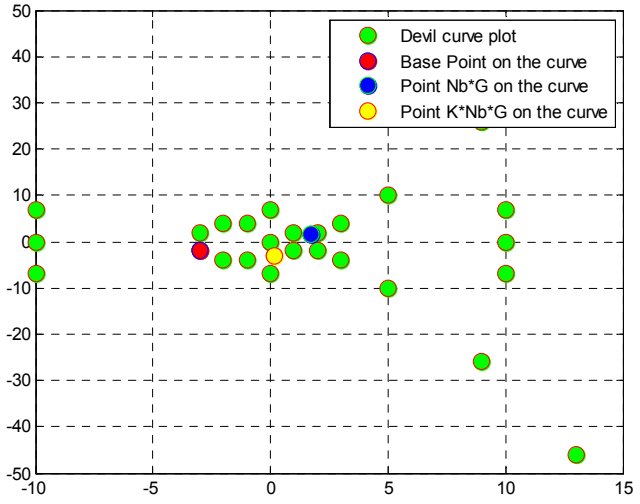

Figure 5. *Graph generated by the polynomial $y^4-4y^2-x^4+81x^2=1 \bmod 53$ where a, b are 2, 9 respectively [12].*

Example
Consider the random points on the above curve where
$b= (40, 4)$
$r= (6, 8)$
Select the two prime numbers p, q.
$p=3$
$q=11$
Calculate n, where $n=p \times q$
$n =3 \times 11 =33$
The random number $x= 3$;
H (m) =3;
The value $H (m)$ obtained from the DICOM header.
According to the modular arithmetic properties
$(b_x,b_y)^x x (c_x,c_y) =1 \bmod n$
$(40,4)^3 x(c_x,c_y) = 1 \bmod n$
$40^3 \times c_x= 1 \bmod 33$
Therefore $c_x =28$
$4^3 \times c_y= 1 \bmod 33$
Therefore $c_y= 16$
$(c_x,c_y) =(28,16)$
$y = r^x \bmod 33$
$y=(6,8)^3 \bmod 33$
$y=(18,17)$
Signature:
$(s_x,s_y)=r \times b^{H(m)} \bmod n$
$(s_x,s_y)=((6,8) \times (40,4)^3) \bmod 33$
$(s_x,s_y) = ((6,8) \times (13, 31)) \bmod 33$
$(s_x, s_y) = (12, 17)$
$(s_x,s_y)^x \times (c_x,c_y)^{H(m)} =(12,17)^3 \times (28,16)^3$
$=(18,17)$

Random points is generated through devils curve which provides complexity in generating random points, Random points in this quartic curve depends on selecting *(a, b)* points, order of the curve. *H (m)* is selected from the DICOM header information maintaining authenticity of each transmission [13, 14].

6. Conclusion

The medical image data can be accessed by the third party and altered the contents of the data during the transmission. To prevent the unauthorized access by the third party the source and destination entity should be authenticated. A digital signature can be generated from a digital media file and appended to DICOM header to be used for authentication and transmitted over a secure channel. At the receiver, the header is received and verified for the signature. If the signature matches then the data transmitted by authorized entity else data transmission done by fraudulent peer. The experiential results proved the correctness and the verification which confirm the storage of signature field lesser compared to conventional methods and more authenticated. The algorithm implemented and tested for various DICOM images.

References

[1] Santhosh B, Dr. K Viswanath, “Review on Medical Image Processing”, Volume 435 of the series Advances in Intelligent Systems and Computing, pp 531-537, Springer, Jan2016.

[2] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo M. Eghan3, Nii Narku Quaynor “A Security Technique for Authentication and Security of Medical Images” in Health Information Systems.

[3] William Stallings, "Cryptographyand Network Security" in Principles and Practices, Prentice Hall, 2003.

[4] Kamal kumar Agrawal, Ruchi Patira, Kapil Madhur,” A Digital Signature Algorithm based on xth Root Problem”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 11, November 2012.

[5] Vanstone, S. A., 2003. Next generation security for wireless: elliptic curve cryptography. Computers and Security, vol.22, No. 5.

[6] Aqeel Khalique, Kuldip Singh, Sandeep Sood” Implementation of Elliptic Curve Digital Signature Algorithm” International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010.

[7] A. Umamageswari I, G. R. Suresh,” Novel Algorithms for Secure Medical Image Communication Using Digital Signature with Various Attacks”, Fifth IEEE International Conference on Advanced Computing (ICoAC) 2013.

[8] Cundy, H. and Rollett, A. Mathematical Models, 3rd ed. Stradbroke, England: Tarquin Pub., p. 71, 1989.

[9] Gray, A. Modern Differential Geometry of Curves and Surfaces with Mathematica, 2nd ed. Boca Raton, FL: CRC Press, pp. 92-93, 1997.

[10] Aqeel Khalique, Kuldip Singh, Sandeep Sood,” Implementation of Elliptic Curve Digital Signature Algorithm, International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010.

[11] http://www.2dcurves.com/quartic/quarticd.html.

[12] Cramer, G. Introduction a l'analyse des lignes courbes algébriques. Geneva, p. 19, 1750.

[13] Interpolation and approximation of polynomials by Philips, G. M. ISBN: 978-0-387-00215-6http://www. springer.com/978-0-387-00215-6.

[14] Ali Al-Haj1, Gheith Abandah, Noor Hussein,”Crypto-based algorithms for secured medical image transmission”, IET journal, ISSN 1751-8709.