International Journal of Electrical Sciences & Engineering (IJESE)
Online ISSN: 2455 6068; Volume 1, Issue 1; January 2016 pp. 19-18

A Robustic Technique to Encrypt Medical Images using Bernstien Polynomial over Prime Field

Smitha Sasi[1], Santhosh B.[2]

[1,2]*Assistant Professor*
Department of Telecommunication Engineering
DayanandaSagar College of Engineering
[1]*smitha.sasi24@gmail.com,* [2]*santhoshmehtre@gmail.com*

Abstract: **Medical image processing techniques requires continuous improve quality of services in health care industry. In the real world huge amount of information has to be processed and and transmitted digitally. Confidentiality and authentication to the transmitted medical images is important in health industry. This work proposed an efficient polynomial based public key cryptographic technique for secured transmission of medical image.**

Keywords: **Medical Image Processing, Bernstien Polynomial, Encryption, Decryption.**

1. INTRODUCTION

Today's world the responsibility of medical institutions is to keeping patients' medical records in secured manner. The Physician or the institution should not to unveil any therapeutic data uncovered by a patient or found by a doctor regarding the treatment of a patient to any unapproved individual. Exchanging restorative information from a medicinal database focus to another without applying any cryptographic systems means low level of security for patients. Therapeutic data transmission has expanded with the utilization of telemedicine. Telemedicine is imperative on the grounds that it empowers conferences by remote authorities, misfortune free and quick accessibility of individual patient data, and enhanced correspondence between accomplices in a medicinal services framework. So the therapeutic information must be classified while transmission.

Secrecy implies that just the qualified clients have admittance for the data and this can be accomplished utilizing encryption. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication path. Cryptographic algorithms can be implementing on symmetric key or asymmetric key systems. In the symmetric key crypto system same key used for both decryption and encryption. A drawback of symmetric key cryptography is that the two gatherings sending messages to one another must consent to utilize the same private key before they begin transmitting secure data. In people in general key cryptosystem open key is utilized to encode the information on sender side and private key on the collector side to decode the information. The essential point of interest of open key cryptography is expanded security and accommodation, private keys never should be transmitted or uncovered to anybody. Open key calculation like RSA the fundamental test is the representation of plain content as a whole number. This paper proposes the polynomial based cryptographic method where the plain text represents as points based on polynomial. The mathematical computation is effective in Bernstein polynomial method. So this paper proposes Bernstein polynomial cryptographic technique.

2. BERNSTIEN POLYNOMIAL

In the scientific field of numerical investigation, a Bernstein polynomial, named after Sergei Natanovich Bernstein, is a polynomial in the Bernstein shape, that is a straight mix of Bernstein premise polynomials. A numerically stable approach to assess polynomials in Bernstein structure is de Casteljau's calculation.

The n + 1 Bernstein basis polynomials of degree n are defined as $n(f, t)=\sum_{r=0}^{n} f\left(\frac{i}{n}\right) nc_i t^i (1-t)^{n-i}$

Where nc_i is a binomial coefficient.

The Bernstein basis polynomials of degree n form a basis for the vector spaceΠn of polynomials of degree at most n.
The coefficient nc_i obtained from Pascal's triangle. The exponent on the (1-t)th term decrease by one as i increases.

- The Bernstein polynomials of degree 1 are

  B0, 1(t) = 1-t

  B1, 1(t) = 1-t

can be plotted for 0<t<1 as shown in fig 1

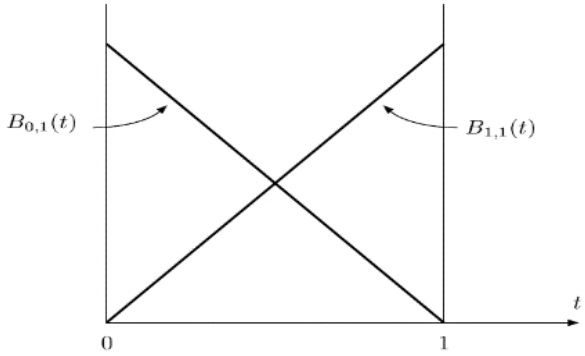

Fig. 1. linear bernstienpolynomail

- Bernstein polynomial of degree 2 are

  B0, 2(t) = $(1-t)^2$
  B1, 2(t) = 2t(1-t)
  B2, 2(t) = t^2

and can be plotted for 0<t<1 as shown in fig 2

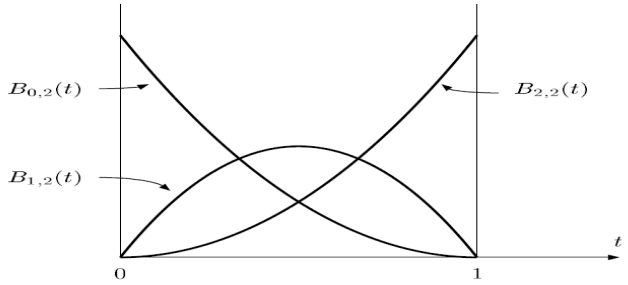

Fig. 2. Quadratic Bernstein polynomial

- Bernstein polynomial of degree 3 are

  B0, 3(t) = $(1-t)^3$
  B1, 3(t) = $3t(1-t)^2$
  B2, 3(t) = $3t^2(1-t)$
  B3, 3(t) = t^3
  and can be plotted for 0<t<1 as shown in fig 3

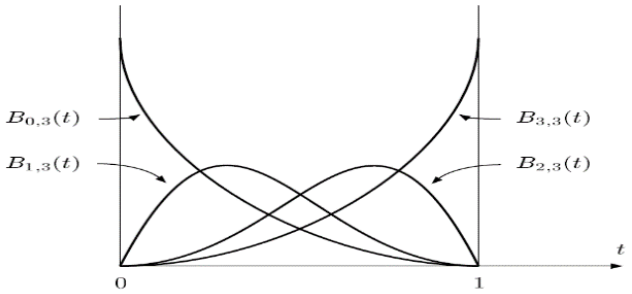

Fig. 3. ternary Bernstein polynomial

A. Mathematical model of polynomial of higher degree

Any of the lower-degree Bernstein polynomials (degree < n) can be communicated as a straight blend of Bernstein polynomials of degree n. Specifically, any Bernstein polynomial of degree n−1 can be composed as a direct mix of Bernstein polynomials of degree $tB_{i,}\, n(t) = nc_i t^{i}+1(1-t)^{n-i}$

$= nc_i t^{i+1}(1-t^{)(n+1)-(i+1)}$
$=(nc_i)/(n+1\ c_{i+1}\ )\ Bi+1,\ n\ +1(t)$
$=i+1/n+1\ Bi+1,\ n\ +1(t)$
$(1-t)Bi,\ n(t) = nc_i ti(1-t)n-+1-i$
$=(nc_i)/(n+1\ c_i)\ Bi,\ n\ +1(t)$
$=n-i+1/n+1\ Bi,\ n\ +1(t)$

$1/\ (nc_i\ )Bi,\ n(t)+1/(n+1\ ci)\ Bi+1,\ n\ (t)= t_i(1-t)n—i+\ ti+1(1-t)n—(i+1)$
$= ti(1-t)n—i-1((1-t)+t)$
$= ti(1-t)n—i-1$
$=1/\ (n-1c_i\ )(Bi,\ n\ -1(t))$

3. PROPOSED ALGORITHM

The general form of the Bernstein polynomial is $n(f, t)=\sum_{r=0}^{n} f\left(\frac{i}{n}\right)nc_i\, t^{i}(1-t)^{n-i}$

When n=5; this polynomial is quintic polynomial.

The general form to check the given number is prime number $p=n^2-n+41$.
Generate (x, y) points based ion the degree of the polynomial.
map those points on to text.
Encryption:

Step 1:

Choose (Kp_u, kp_r) and (α_1, α_2) are the pairs of the keys
Where K_u is the public key and k_r is the private key.

Step 2:

Choose the secret reference point on the curve based on quintic polynomial

Step 3:

Choose the plain text point (P_x, P_Y) is the pixel point on medical image

Step 4:

Perform (P_x, P_Y) /(α1, Kp_u) mod(n-n+41)=(a, b) this is the another point on the curve. (perform point division operation)

Step5:

(a, b)/secret reference point mod(n^2-n+41)=(Cx, C_Y) this is the cipher text.
Cipher text will be the point on the curve. So the final resultant curve which contains all the point of cipher text transmit to receiver side.

Decryption:

On receipt of the cipher text points receiver starts perform decryption.

Step 1:

Perform (Cx, Cy) (secret reference point) mod (n^2-n+41)=(a_1, b_1)
(secret reference point will be exchanged between two parties by using any secure key exchange algorithm)

Step 2:

Perform (a_1, b_1)/(α_2, K_r) mod (n^2-n+41)= (P_X, P_Y) this is the plain text value, if receiver use proper private key.
Relation between Kp_u and Kp_r is
$Kp_r=n[(b-nK_u)/(1-n) +b(1-n)/n]$ mod n^2-n+41.
The relation between α_1, α_2 is
$\alpha_2=n[a-n\alpha_1)/(1-n)+a(1-n)/n)]$ mod n^2 -n+41.

4. RESULT

Encryption:

(P_x, P_y)=(4, 43) is the pixel on image
(α_1, Kp_u)=(7, 3)
(a, b)=(P_x, P_y)/(α_1, Kp_u)mod(n^2-n+41)=(4, 43)/(7, 3)mod(n^2-n+41)
(a, b)=(19, 26)
(a, b)/secret reference point=(C_X, C_Y)

Secret reference point=(2, 7)
(19, 26)/(2, 7) mod(n^2-n+41)=(56, 53)

Decryption:

(C_X, C_Y)x(secret reference point)mod(n^2-n+41)=(a1, b1)
(56, 53) x (2, 7) mod(n2-n+41)=(19, 26)
(a1, b1)/(α_2, Kp_r) mod(n^2-n+41)= (P_X, P_Y)

From the relation;
$Kp_r=n[(b-nKp_u)/(1-n) +b(1-n)/n]$ mod n^2-n+41. $\alpha2=n[a-n\alpha_1)/(1-n)+a(1-n)/n)]$ mod n^2 -n+41. ($\alpha2$, K_r)=(5, 50)
(19, 26)/(5, 50) mod(n^2-n+41)=(4, 43)

5. CONCLUSION

Bernstein polynomial over prime field based cryptographic approach provides security and reduces computational complexity. This cryptographic method can implement over medical images to protect the patient databases in confidential manner.compared to other public key crypto methods like RSA and ECC, this method reduces the computational complexity, and supports any order of n, higher order n leads to improve security.

6. ACKNOWLEDGEMENT

I would like to express my gratitude to Dr A R Aswatha who motivated us to write this article and also thankful to all faculties of Telecommunication Department for their support.

REFRENCES

[1] H. Caglar and A. N. Akansu, *"A Generalized Parametric PR-QMF Design Technique Based on Bernstein Polynomial Approximation,"* IEEE Transactions on Signal Processing, vol. 41, no. 7, pp. 2314–2321, July 1993.

[2] Online geometric modelling notes: *Bernstein; Visualization and graphics research group; department of computer science*, University of California

[3] http://mathworld. wolfram.com

[4] William Stallings, "*Cryptographyand Network Security*", Principles and Practices, 3rd Edition, Prentice Hall 2003.

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

[6] The Encyclopedia of design theory: Galois fields by Peter J. Cameron May 30, 2003.

[7] Error Control Coding by Shu Lin, Daniel J Costello; 2nd edition.

[8] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud "Performance evaluation of symmetric encryption algorithms" Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765.

[9] Dr. SudeshJakhar" Comparative analysis between DES and RSA algorithms" IJARCSSE Volume 2, Issue 7, July 2012, pg no. 386-390.