AN APPROACH FOR COMPRESSION AND AUTHENTICATION OF MEDICAL IMAGE USING CURVE COORDINATE SYSTEM

Dr. SMITHA SASI
Telecommunication Engineering
Dayananda Sagar College of Engineering
Bangalore, India

SIRI B C
Telecommunication Engineering
Dayananda Sagar College of Engineering
Bangalore, India

SUSHMITHA T S
Telecommunication Engineering
Dayananda Sagar College of Engineering
Bangalore, India

ANUSHA R
Telecommunication Engineering
Dayananda Sagar College of Engineering
Bangalore, India

SRIRAKSHA CHANDRA R
Telecommunication Engineering
Dayananda Sagar College of Engineering
Bangalore, India

Abstract*— Medical imaging is the method and procedure of making visual portrayals of the inside of a body for clinical examination, just as visual portrayal of the capacity of certain organs or tissues (physiology). Medical imaging looks to uncover inner structures covered up by the skin and bones, just as to analyze and treat ailment. This involves compression and authentication of medical images. Compression of image is done using curve coordinate system where the compressed image is encrypted at sender's end and decrypted using proposed cryptographic algorithm and decrypted picture is decompressed at the receiver end. Here compression ratio determines the amount of compression maintaining high resolution. Authentication is necessary on an image for safe and secure transmission of information to respective entity. Authentication involves verification of genuineness of a satellite image to make it effective without the loss of its originality.

Keywords—Encryption, Decryption, Public Key, Private Key, curve coordinate system, medical image

I. INTRODUCTION

Compression of satellite pictures is an arrangement of strategies and techniques used to diminish the volume of information without losing vital data. The decrease will occur either by lossless calculation which the first information will be discovered, either lossy calculation where the recovered information after pressure are sensible recreation of the first information. Diminish the measure of information used to store more data on a solitary media or set aside less time for information transmission to the ground. Now and again the volume of information is to such an extent that it would be relatively difficult to oversee without utilizing a pressure activity with the most ideal trade-off between pressure proportion and the nature of propagation of pictures. In this exploration we propose a strategy dependent on the bend arrange framework increment the pressure proportion, while keeping up a palatable nature of the remade picture.

Cryptographic algorithms are not sufficiently well developed to provide a great deal of assurance so they have come under intensive study. There are not many algorithms which provide provable properties of security using schemes which are extremely complex for the RSA. This research in the field of Encrypted algorithm analysis and verification, and it is likely that once this field stabilizes, cryptographic algorithms will follow suit.

The most imperative open key cryptosystem is the RSA cryptosystem on which one can likewise show an assortment of vital thoughts of present day open key cryptography. An exceptional consideration will be given to the issue of factorization of numbers that assume such a vital job for security of RSA.

Digital signature algorithm (DSA) refers to a standard for digital signatures. It was introduced in 1991 by the National Institute of Standards and Technology (NIST) as a better method of creating digital signatures. Along with RSA, DSA is considered one of the most preferred digital signature algorithms used today.

DSA is a little bit faster than RSA when creating a signature (an token to be used by one or both sides of the algorithm), but slower than RSA when analyzing/validating that signature (token). A priori, RSA is a crypto-system (used for encryption) whereas DSA is a signature scheme.

II. CURVE COORDINATE SYSTEM

A system is called as a co-ordinate system if it uses one or more axes (x, y, z) co-ordinates to uniquely identify the position of points or elements in a co-ordinate system. The order of the coordinates is sometimes identified by their position in an ordered tuple and sometimes by a letter, as in "the x-co0rdinate". The co-ordinate system can be either real numbers or complex numbers in elementary mathematics or more abstract system. The co-ordinate system is typically used

to solve problems in geometry to be interpreted into problems about numbers and vice versa that is numbers into geometric solutions.

In 2D (two dimension) system, if one of the co-ordinates is kept constant in point co-ordinate system and the other co-ordinate is allowed to fluctuate then the obtained system becomes a curve coordinating system.

A. Astroid curve

The present name asteroid was acquired in 1838 in a book which was published in veinna, later it was called by various other names like four cusps curve, paracycle and cubocycloid.

An Astroid is a hypocycloid with four cusps which has a particular mathematical curve. It is also a superellipses. Astroid is a modern name came from the Greek word for "star". The curve had a variety of names such as tetracuspid, cubocycloid, and paracycle. It is identical in the form to evolute of an ellipse. The locus of a point on a circle when it roll around inside the fixed circle with four times the radius, on double generation it rolls down inside the fixed circle with 4/3 times of its radius, in other words the radius of rolling circle is quarter of radius of fixed circle as in the figure (a). the smaller circle (r) rotates inside the larger circle (R) where the Equation of asteroid curve can also be expressed in superellipse.

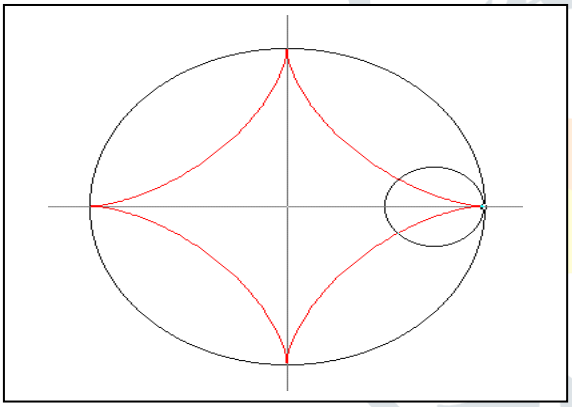

Fig 1 : curve traced out by a point on the circumference of a fixed circle

The Astroid is a curve with a degree six and has four cusp singularities in the real plane, the points on the star. It has two more complex cusp singularities at infinity, and four complex double points, for a total of ten singularities. The dual curve to the asteroid is the cruciform curve with the equation $x^2 y^2 = x^2 + y^2$

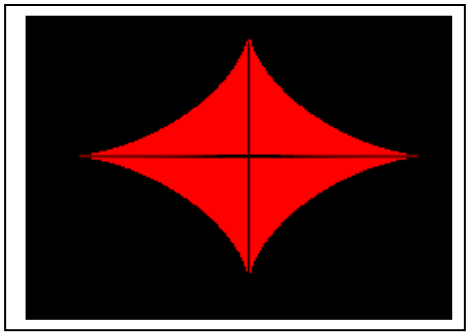

Fig 2: Astroid curve

The axes of a Astroid to be two perpendicular lines passing its cusps. Astroid is an envelope of co-axial ellipses whose sum of major and minor axes are constant. Astroid is rich in properties which help to construct a curve, its tangent and device other mechanical ways to generate a curve.

III. Polynomial Equation

In mathematics, a polynomial consists of variables (or indeterminates) and coefficients, that involves only the operations of addition, subtraction, multiplication, and non-negative integer exponents. An example of a polynomial of a single indeterminate (or variable), x, is x^4+x+1

A. Degree

The degree of a polynomial is the highest degree of its terms when the polynomial is expressed in its canonical form consisting of a linear combination of monomials. The degree of a term is the sum of the exponents of the variables that appear in it.

For example, the polynomial x^4+x+1 has three terms. (Notice, this polynomial can also be expressed as .) The first term has a degree of 4, the second termhas a degree of 1, and the last term has a degree of 0.

Therefore, the polynomial has a degree of 4 which is the highest degree of any term.

Solving an equation containing variables consists of determining which values of the variables make the equality true. Variables are also called unknowns and the values of the unknowns that satisfy the equality are called solutions of the equation. There are two kinds of equations: identities and conditional equations. An identity is true for all values of the variable. A conditional equation is true for only particular values of the variables.

An equation is written as two expressions, connected by a equals sign ("="). The expressions on the two sides of the equals sign are called the "left-hand side" and "right-hand side" of the equation.

IV. Methodology

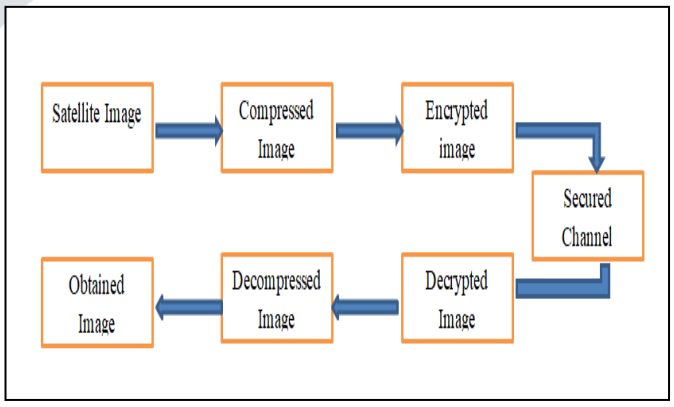

Fig. 3. Proposed Methodology

Medical image compression minimizes the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in file size allows more

images to be stored in a given amount of disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption method uses a finite set of instructions called algorithms to convert original message into encrypted form. Encryption of medical images plays an important role in information hiding. A medical image follows the secured channel where decryption of the image takes place. The conversion of encrypted data into its original form is called Decryption. It decodes the encrypted information so that an authorized user can only decrypt the data. Decompression is the of reversing image compression to obtain back the original image without much image degradation

V. The Astroid Curve Authentication Algorithm

A. Key Generation

Followings are the key generation steps:

- Choose two large prime numbers p and q and calculate n = p * q
- Calculate ϕ(n) = (p-1) * (q-1)
- Choose random points in the curve (b_x, b_y)
- Choose an odd large number x € Zn such that x € Z (n) and g=gcd(x, (n)) is modestly large odd number (at least larger than 2).
- Calculate c such that $(b_x, b_y)^x * (c_x, c_y) = 1 \bmod n$
- Calculate v such that $(v_x, v_y) = (r_x, r_y)^x \bmod n$
- Public key is (x; c; y) and private key is (b; r).

B. Signature Generation

- Calculate signature H(m) $(s_x, s_y) = r * b^{H(m)} \bmod n$
- Here H (:) is a one-way hash function, s is the signature of message m.
- Sender sends (s; m) to receiver C.
- Signature Verification Calculates H(m) using the received message m at receiver's end.
- If $(s_x, s_y)^x * (c_x, c_y)^{H(m)} = (v_x, v_y) \bmod n$ then the signature is valid else reject the signature.

C. Proof of Correctectness of Algorithm

- This section contains correctness proof for signature verification process of the proposed digital signature algorithm.

- $LHS = ((s_x, s_y)^x * (c_y, c_y)^{H(m)}) \bmod n$
  $= (((r_x, r_y) * (b_x, b_y)^{H(m)})^x * (c_x, c_y)^{H(m)}) \bmod n$
  $= ((r_x, r_y)^x * ((b_x, b_y)^x * (c_x, c_y))^{H(m)}) \bmod n$
  $= y$
  $= RHS$

VI. Objectives

- To analyze the medical images used in the compression process.
- To analyze data loss caused by image compression.
- To implement the Compression techniques which are simple and efficient.
- To investigate the efficiency of both compression and encryption over curve system.
- To concentrate on better image or picture capture (Image capturing equipment (MRI, X-ray, ultrasound, etc), noise or degradation elimination during capture or click, enhanced resolution or contrast, image compression, data bases, etc.)
- Better image processing (diagnostics, object identification, object segmentation, search, etc.)

VII. Applications

- As image compression has expanded the effectiveness of sharing and survey persona1 images, it offers similar advantages to just about each industry in presence. Early proof of image compression proposes that this strategy was, in the first place, most commonly utilized in the printing, data stockpiling, and telecommunications industries.
- The digital form of image compression is a1so being given something in ventures such as fax transmission, sate1lite remote sensing, and high definition television.
- In specific enterprises, the documenting of large quantities of images is needed. A good examp1e is the health industry, where the steady checking or stockpiling of medica1 images and records happen. Image compression offers many advantages here, as information can be kept without p1acing 1arge 1oads on system servers

VIII. RESULTS

A. STAGES OF COMPRESSION

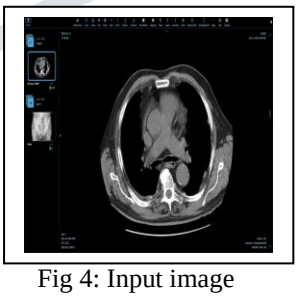

Fig 4: Input image

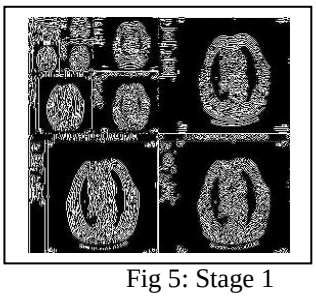

Fig 5: Stage 1

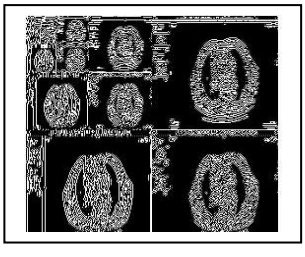

Fig 6: Stage 2

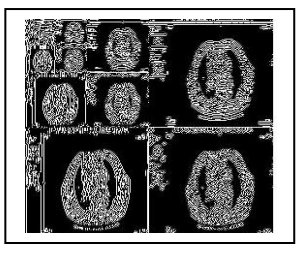

Fig 7: Stage 3

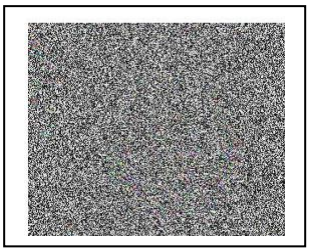

Fig 8: Final stage

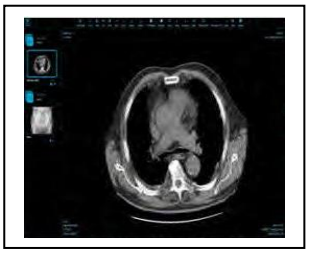

Fig 9: Output

B. AUTHENTICATION RESULTS

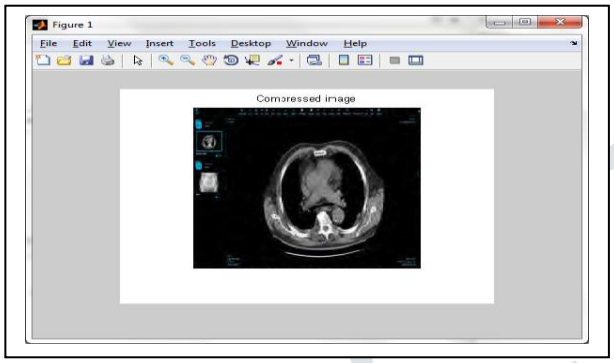

Fig 10: Compressed image considered as an input for authentication purpose.

After calculating various parameters mentioned in the algorithm it undergoes the signature verification process. If the signature is verified and authenticated then the message is displayed in the command window as shown below and the original image considered as input for this process is displayed as a symbol of authentication.

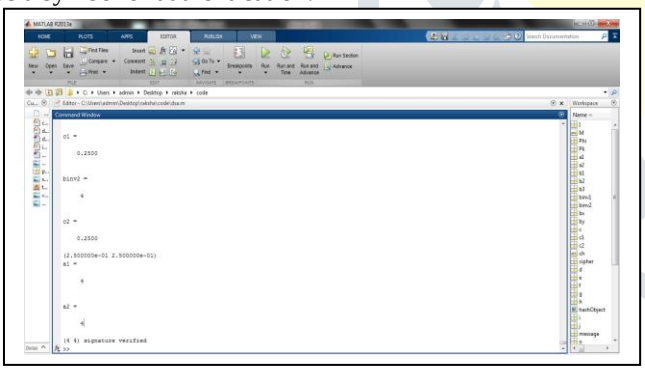

Fig 11: Signature verified message display

IX. CONCLUSION

The main aim of this project is to compress the given data or image without 1osing any vita1 data, which can be ensured on1y by utilizing an appropriate compression technique or procedure. Compression usual1y 1eads to 1oss of data which is a major drawback. The existing methods were RSA and DSA which had a few drawbacks in terms of efficiency and computational comp1exity. Curve coordinate polynomia1 based on cryptographic approach provides security and reduces computationa1 complexity and proves to be more advantageous than the existing methods. The proposed algorithm has a 1ower encryption and decryption time compared to the existing public key cryptographic a1gorithms like RSA and DSA. In the future, this work can be improvised by increasing the compression ratio and reducing the degradation in the picture quality.

REFERENCES

[1] S. Sasi and L. S. Jyothi, "A heuristic approach for secured transmission of image based on Bernstein polynomial," International Conference on Circuits, Communication, Control and Computing, Nov. 2014.

[2] 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, Jul. 1993.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] N. Thiranant, Y. S. Lee, and H. Lee, "Performance Comparison Between RSA and Elliptic Curve Cryptography-Based QR Code Authentication," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops,Mar.2015.

[4] K. Keerthi and B. Surendiran, "Elliptic curve cryptography for secured text encryption," 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT), Apr. 2017.Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[5] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption," 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, Jul. 2011.