

Design and Implementation of Compressed Medical Data over an Authenticated Secured Channel



Santhosh B., Viswanath K.

Abstract: Ideally, secure transmission of medical image data is one of the major challenges in health sector. The National Health Information Network has to protect the data in confidential manner. Storage is also one of the basic concern along with secure transmission. In this paper we propose an algorithm that supports confidentiality, authentication and integrity implementation of the scrambled data before transmitting on the communication medium. Before communication the data is compressed while keeping data encrypted. The research work demonstrate with simulation results. The results shows that the proposed work effectively maintains confidentiality, authentication and integrity. The experimental results evaluated medical image quality like PSNR, MSE, SC, and NAE etc.

Keywords: Devil's Curve, Encryption, Decryption, Compression, DSA, Prime Number.

I. INTRODUCTION

The appearance of data innovation in the therapeutic world different radiological modalities produce an assortment of advanced medicinal documents regularly informational collections and images. The documents which contains data known for digital data set should be protected from unwanted modification of these contents, specifically they contain imperative information or data. Thus, the safety and authentication of data are important whenever the exchanges of data happen. The Data of a digital image is easily accessed and modified while being exchanged through electronic correspondence and data frameworks. Thus image protection and authentication have become a vital Issue in recent years. A digital signature could be generated from a media file and is scrambled as an additional file added to media and to be used for authentication [1]. For protecting the confidential information digital signature and data encryption techniques plays a significant role in the protection of data.

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Channel Santhosh B., Pursuing Ph.D., Department of Telecommunication Engineering, Visvesvaraya Technological University Belgaum, India.

K. Viswanath, Professor, Siddaganga Institute of Technology, Tumakur, Karnataka, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

The significance of a verified trade of medical images has demonstrated the path for universal social importance as to distribute exceptional principles with restorative information security issues. DICOM (Digital Imaging and Communication On Medicine) is a standard which protects the data.

The standard gives the rules and guidelines to health care experts and substances to accomplish three administrations 1) confidentiality 2) integrity 3) authentication.

Viability of the proposed algorithm is assessed and exhibited through constant analysis and utilizing a criteria set of DICOM images [7].

II. PROPOSED ALGORITHMS

This paper proposed design and implementation of compression crypto based algorithm provides confidentiality of the data and verify authenticity, integrity of the input images. The medical data is the input to the proposed algorithm and asymmetric keys are generated and applied on the DICOM images, Signature is also applied for authenticity of the input images. The designed algorithms addresses data confidentiality, integrity of the data and authenticity of DICOM header and Pixel of medical images with successful functions. The functions are:

- 1) Devil's co-ordinate based compression
- 2) Quartic Digital Signature Algorithm
- 3) Devil's public key cryptosystem

This algorithm provides asymmetric encryption, digital signatures and hashing to maintain integrity, confidentiality and authenticity for both the header and pixel data of medical images [8]. Devil's curve are incorporated with the utilization of the pixel data and digital confidential features which the curve introduces the Authenticated tag and cipher pixel data simultaneously. Using the hash function the initialization vector and encryption keys are introduced. The authentication tag is then signed by Devil's curve DSA. The public key cryptography and signature creation are described below [2,3].

III. DEVIL'S PUBLIC KEY CRYPTOSYSTEM:

Encryption:

Step1: select two pairs of points on the curve (KU, KR) and (β_1, β_2)



Step2: Select a point on the curve based quartic polynomial.

Step3: consider a pixel point (DX, DY) on the input image.

Step4: By applying point division operation on $\frac{(DX, DY)}{(\beta 1, KU)} \bmod 53 = (s, t)$

Step5: calculate ciphertext by $\frac{(s, t)}{(secret\ key)} \bmod 53 = (RX, RY)$

3.2. Decryption:

After receiving the cipher data, decryption steps are as follows:

Step1: Perform $(RX, RY)(secret\ key) \bmod 53 = s1, t1$
secret key is shared between both the parties.

step2: Perform $\frac{(s1, t1)}{(\beta 2, KR)} \bmod 53 = (DX, DY)$ is the pixel value.

Relation between (KU, KR)

$$KR = n \left[\frac{t-pKU}{1-p} + \frac{t(1-p)}{p} \right] \bmod 53.$$

The relation between $(\beta 1, \beta 2)$

$$\beta 2 = p \left[\frac{s-p\beta 1}{1-p} + \frac{s(1-p)}{p} \right] \bmod 53.$$

Encryption Example:

$(DX, DY) = (28, 35)$ Is the pixel on the input medical image

$$(\beta 1, KU) = (7, 3)$$

$$(s, t) = \frac{DX, DY}{(\beta 1, KU)} \bmod (n^2 - n + 41) = (50, 13)$$

$$\frac{(s, t)}{(secret\ key)} = (RX, RY) \{ Secret\ reference\ point = (2, 7) \}$$

$$\frac{(50, 13)}{(2, 7)} \bmod (n^2 - n + 41) = (17, 42)$$

$$((RX, RY) * (secret\ reference\ point)) \bmod (n^2 - n + 41) = (s1, t1)$$

$$(17, 42) * (2, 7) \bmod (n^2 - n + 41) = (50, 13)$$

$$\frac{s1, t1}{\beta 2, KR} \bmod (n^2 - n + 41) = (DX, DY)$$

From the relation KR, 2:

$$(\beta 2, KR) = (15, 48)$$

$$\frac{50, 13}{15, 48} \bmod (n^2 - n + 41) = (28, 35)$$

IV. DEVIL'S CO-ORDINATE BASED COMPRESSION

The proposed degree of the polynomial generate the points (s,t). Generate the image for the devil's curve based polynomial coordinate elements [4,5]. Step wise procedure are as follows:

1. Let II be an input image and DI is the devil's image based polynomials [14,15].
 2. The II is divided by DI and compress the image CI by $(II[s,t]/DI[s,t]) \bmod 255$. Using PDF (Point Division Method). Therefore $CI = II + n(DI - II) \bmod 255$
 3. Resultant compressed image is transmitted over a secured channel.
 4. Decompression of the decrypted image to recover original image is :
- $$DeI[s,t] = (CI[s,t] * DI[s,t]) \bmod 255$$
- $$DeI(s) = (CI(s) - n * DI(s) / (1 - n)) \bmod 255$$
- $$DeI(t) = (CI(t) - n * DI(t) / (1 - n)) \bmod 255$$

The prime numbers should be in the range of n is $0 < n < 255$

V. QUARTIC DIGITAL SIGNATURE ALGORITHMS BASED ON DEVIL'S CURVE:

The authentication of message secures two parties exchanging messages from third party. However, the two parties against each other cannot be protected. Based on the complexity of the 10th root a digital signature methodology is developed.[17]. The algorithm is as follows:

Key Generation:

Key generation steps are as below:

Select two large prime numbers p and q. find $n = p * q$

Calculate $\phi(n) = (p - 1) * (q - 1)$

Select random points in the devils curve (g_x, g_y)

Select an odd large number $X \in \mathbb{Z}_n$ such that $X \notin \mathbb{Z}(n)$ and $g = \gcd(X; (n))$ is large (> 2).

Find C such that $(g_x, g_y) * (h_x, h_y) = 1 \bmod n$

Calculate V such that $(u_x, u_y) = (q_x, q_y) \bmod n$

Signature Generation:

Calculate signature $H(m)(s_x, s_y) = q * g^{H(m)} \bmod n$ Here

H (:) is a one way hash function. s is the signature of message m.

Sender sends (s; m) to receiver. C.

Signature is Verified by Calculating H(m) using the received message m at receiver's end.

If $(s_x, s_y) * (h_x, h_y)^{H(m)} (u_x, u_y) \bmod n$ then the signature is valid or else reject .

Proof of correctness of the algorithm:

This section verifies signature proposed digital signature algorithm:

$$\begin{aligned} \text{LHS} &= (((s_x, s_y)^x * (g_x, g_y)^{H(m)}) \bmod n \\ &\quad (((q_x, q_y) * (g_x, g_y)^{H(m)^x} * (h_x, h_y)^{H(m)}) \bmod n \\ &\quad (((q_x, q_y)^x * (g_x, g_y)^x * (h_x, h_y)^{H(m)}) \bmod n \\ &= y = \text{RHS} \end{aligned}$$

Example:

$$y^4 - 4y^2 - x^4 + 81yx^2 = 1 \bmod (n^2 - n + 41)$$

where n =4, for quartic curve degree is 4.

$$\text{We get } y^4 - 4y^2 - x^4 + 81yx^2 = 1 \bmod 53$$

where a=2 and b=9 The curve points generated are

(13,4), (40,4), (5,7), (48,7), (6,8), (47,8), (25,11), (28,11), (2,15), (17,15), (7,3) etc.

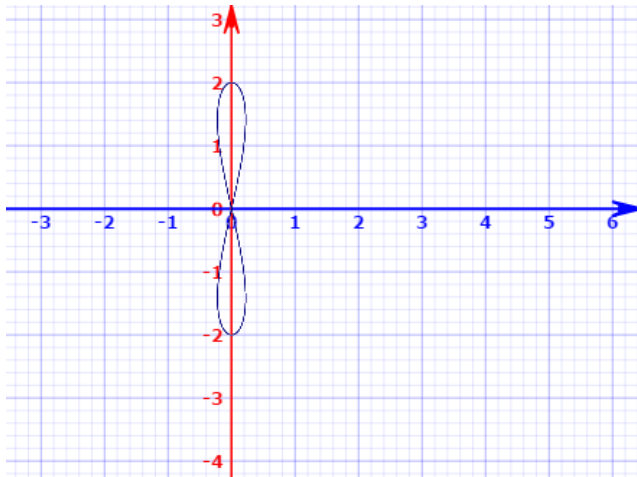


Fig.1.1 Graph generated by the polynomial $y^4 - 4y^2 - x^4 + 81yx^2 = 1 \mod 53$ where a and b are 2,9 respectively.

Consider the random points on the above curve $b = (40,4)$ & $r = (6,8)$

Prime numbers $p=3$ $q=11$

$n=p \times q = 3 \times 11 = 33$

The random number $x = 3$;

$H(m) = 3$;

$$(g_x, g_y) * (h_x, h_y) = 1 \mod n$$

$$(40,4) * 3 * (h_x, h_y) = 1 \mod n$$

$$403 * c_x = 1 \mod 33$$

$$\text{Therefore } c_x = 28$$

$$43 * c_y = 1 \mod 33$$

$$\text{Therefore } c_y = 16$$

$$y = r^x \mod 33$$

$$= (6,8) 3 \mod 33$$

$$= (18,17)$$

Signature:

$$(s_x, s_y) = q * g^{H(m)} \mod n$$

$$(s_x, s_y) = ((6,8) \times (40,4) 3) \mod 33$$

$$= ((6,8) \times (13, 31)) \mod 33$$

$$= (12,17)$$

$$(s_x, s_y) * (h_x, h_y)^{H(m)} = (12,17) 3 \times (28,16) 3$$

$$= (18,17)$$

VI. PROCEDURE TO CREATE SECURED DATA SIGNATURE:

This procedure involves pixels and header information of the input image is encrypted as illustrated in in Fig.1.2

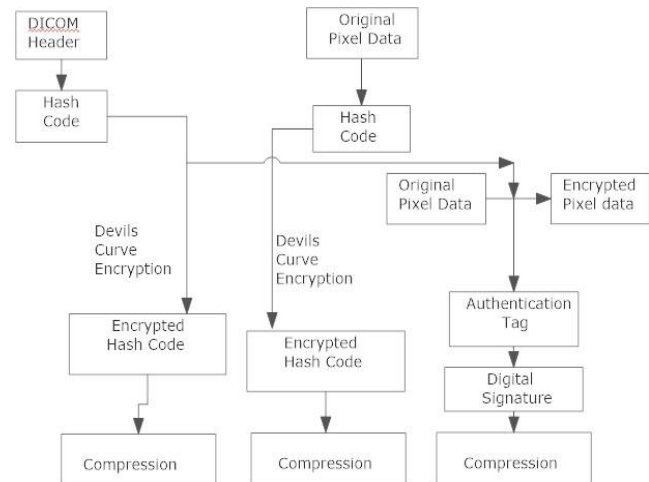


Fig.1.2: Procedure to create secured signature

1. **Data confidentiality of Header:** To integrate in with the application level privacy profile portrayed in PS3.15 DICOM, the methodology peruses every single secret characteristic of the metadata ,encodes their unique qualities utilizing Devil's curve cryptographic system and stores the data in the 'altered traits grouping (0400, 0550)' while supplanting the qualities in the first areas with modified ones. Devil's curve cryptographic method use public key to encrypt the DICOM header. The hash code is calculated by the hash function. Devil's curve cryptographic encodes the hash code and it is stored in the DICOM header which is used to verify at the receiver end. Different DICOM files have different confidential header attributes, and thus the encryption key varies and reduces security risks to avoid introduction of potential vulnerability in the encryption process [9].

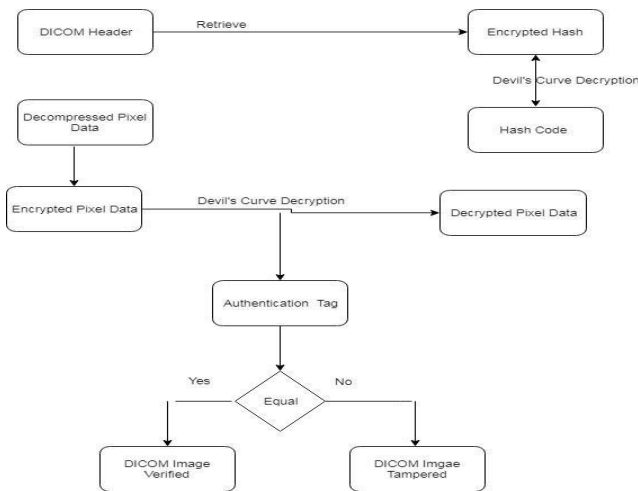
2. **Data authenticity and integrity of Header:** To fetch the header data, the data signed by using private key generated by Devil's curve signature algorithm and this signature is stored in the DICOM header.

3. **Confidentiality of Pixel data:** Devil's curve Cryptographic technique is used to encrypt the pixels. The same encryption algorithm encrypts the header data. But, the hash code is the secret key generated by operating a hash function on the header confidential data. The hash code is encrypted by Devil's curve cryptographic technique and DICOM header holds it for further use at the receiver's end [10,11].

4. **Authenticity and integrity of Pixel data:** The data signed by using private key generated by Devil's curve signature algorithm to authenticate the pixel data. According to the digital signatures profiles described in part PS 3.15 of the DICOM standard; the signature is stored in the DICOM header. The hash code that is encrypted and the encrypted data with signature compressed by Devil's curve compression technique and transmit to the authenticated receiver.

VII. PROCEDURE TO VERIFY SECURED SIGNATURE:

This technique decrypts the partially scrambled DICOM header and the encoded pixel information, and validate their integrity and authentication of the data as shown in Fig. 1.3 described hereafter.



Confidentiality: This research work proposed confidentiality for both data as well as header information. To secure the pixel data, fetch the encrypted hash code of DICOM header's confidential parameters from the metadata and decrypt it using the Devil's curve cryptographic standard. The pixel data is decrypted using decryption key. Devil's curve produce authentication tag of the pixel data.

Devil's curve cryptographic standard decrypts the encrypted hash code of the pixel data. The confidential parameters of the header is decrypted using decryption unscrambled method

i) **Authenticity and integrity:** Authenticity as well as integrity introduced in header as well as data. To fetch the digital signature of the pixel data extract its authenticated tag obtained by hash function using the public key of the sender.

Contrast the extricated tag and the verification tag produced by Devil's curve cryptographic in the previous step. If the two tags match then authenticity and integrity of the pixel data are verified.

To introduce authenticity and integrity in header of the DICOM data, consider digital signature from the DICOM header and extract its authentication tag using the public key of the sending entity.

Contrast the authentication tag with the authentication tag produced by DSA in the last step. If both tags match confidential parameters are verified the authenticity and integrity of the confidential header parameters are verified only if both tags match.

VIII. DATA TRANSMISSION

i) Sender Side Operations:

The sender requests the Application Layer Protocol to transmit the message. Once it receives the message the peer entity initiates the transaction. The transmitter entity fetches the information and before transmission information is encrypted using public key. The data

transmitted to the lower layer and performs the encapsulation. The data packet is transmitted over the IP layer and IP header is concatenated with the data which forms IP datagram and transmits to the Data link Layer. Data Link Layer encapsulates the frames and transmits over the physical medium [12, 13].

Receiver Side Operations:

The Data link layer receiver receives the frame and matches the Ethernet address then it exclude the header and transmits to the Network layer. In the Network layer, the Receiver verifies the destination IP address and protocol field of the transport layer. The protocol field is 17 for UDP. Then datagram is passed through application layer and verifies the application port number, if matches then the data is received and stored in the receiver file store. The Receiver analyzes the metadata in detail if it is same then decryption is performed using private key and data is decompressed.

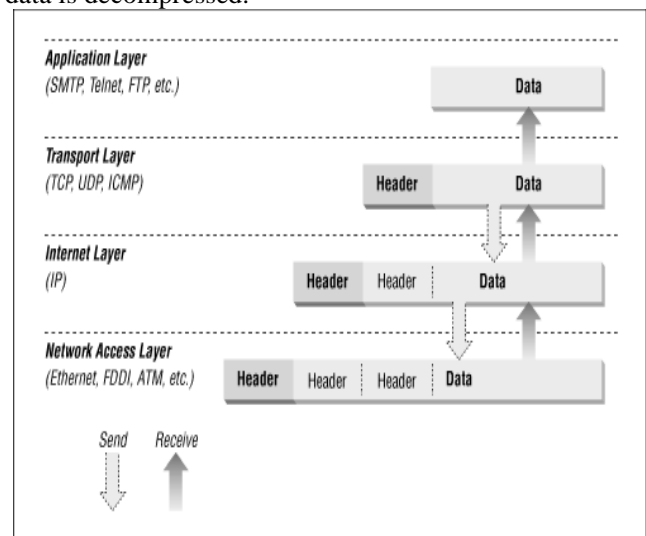


Fig1.4: Data transmission over the IP layers

IX. RESULT AND DISCUSSION

The Table 1.1 explains image measurement quality parameters like PSNR, MSE, NAE and SC .The Results are confirmed for various modalities and tested for the order 4 as well as the key pair (3,25) and (2,5)

The below table provides information about the experimental design, analysis and evaluation of the algorithm. The algorithm implemented in MATLAB and done the following designs on DICOM image. i) Point Generation on Devil's curve ii) Encryption/Decryption on Devil's Image iii) Compression iv) Quartic DSA for authentication.

X. CONCLUSION

Medical imaging is one of the emerging fields of medical electronics, which apply principles of technology in field of health industry. Accuracy in analysis of medical records is as important as reliability of data acquisition process.

The content of a digital image is compressed while being transferred via electronic communication and information systems using Devil's curve systems. A digital signature can be generated from a digital media file and is encrypted as an extra file appended to media and to be used for authentication using curve system based algorithms. The experimental results measured the image quality parameters like MSE, PSNR, SC etc.

REFERENCES

1. A. Umamageswari and G. R. Suresh, "Novel algorithms for secure medical image communication using Digital Signature with various attacks," 2013 Fifth International Conference on Advanced Computing (ICoAC), Chennai, 2013, pp. 152-157. doi: 10.1109/ICoAC.2013.6921943
2. Cramer, G. Introduction a l'analyse des lignes courbes algébriques. Geneva, p. 19, 1750
3. Cundy, H. and Rollett, A. Mathematical Models, 3rd ed. Stradbroke, England: Tarquin Pub., p. 71, 1989.
4. Gray, A. Modern Differential Geometry of Curves and Surfaces with Mathematica, 2nd ed. Boca Raton, FL: CRC Press, pp. 92-93, 1997.
5. Interpolation and approximation of polynomials by Philips, G.M. ISBN: 978-0-387-00215-6
6. <http://www.springer.com/978-0-387-00215-6>.
7. 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.
8. William Stallings, "Cryptography and Network Security" in Principles and Practices, Prentice Hall, 2003.
9. Ali Al-Hajl, Gheith Abandah, Noor Hussein, "Crypto-based algorithms for secured medical image transmission", IET journal, ISSN 1751-8709 Aqeel Khaliq, Kuldip Singh, Sandeep Sood,
10. Implementation of Elliptic Curve Digital Signature Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 2 No.2, May 2010.
11. Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo M. Eghan, Nii Narku Quaynor, A Security Technique for Authentication and Security of Medical Images in Health Information Systems
12. Sasi, S., D. L. Swarna Jayothi, "A Heuristic Approach for Secured Transmission of Image Based on Bernstein Polynomial". – In: Proc. of International Conference on Circuits, Communication, Control and Computing, IEEE, 2013, pp. 312-315.
13. K. Viswanath, J. Mukhopadhyay and P. K. Biswas, "Transcoding in the block DCT space," IEEE International Conference on Image Processing (ICIP 2009), 7-11 Nov 2009, Cairo Egypt, pp. 3685-3688.
14. K. Viswanath, J. Mukherjee, S. Mukhopadhyay and R. N. Pal, "Transcoding: JPEG2000 to JPEG," International Conference on Advanced Computing and Communication (ICACC2007), 9-10 Feb 2007, Madurai-India, pp. 355-358.
15. Z. Xiong, K. Ramchandran, M. T. Orchard, Y.-Q. Zhang, "A Comparative Study of DCT and Wavelet based Image coding: IEEE Transaction on Circuits and System for Video Tech. vol. 9, pp. 692-695, Aug 1999.
16. S. Mallat: A wavelet tour of signal processing, Academic Press. Elsevier. 1998.
17. G.M. Phillips: Interpolation and approximation of polynomials. ISBN: 978-0-38700215-6 <http://www.springer.com/978-0-387-00215-6>.
18. <http://mathworld.wolfram.com>
19. <http://www.2dcurves.com/quartic/quarticd.html>
20. Dr. Sudesh Jakhar "Comparative analysis between DES and RSA algorithms" IJARCSSE Volume 2, Issue 7, July 2012, pg no. 386-390.
21. William Stallings, "Cryptography and Network Security", Principles and Practices, 3rd Edition, Prentice Hall 2003.

information and Embedded Systems from Indian Institute of Technology, Kharagpur, West Bengal, INDIA in 2008. He is currently pursuing the Ph.D. degree in Telecommunication Engineering at Visvesvaraya Technological University Belgaum, INDIA. His research interest includes the development of algorithms for medical image processing, space communication and error control coding techniques. He is the Co-Principal Investigator in the project entitled "Secured file delivery protocol for space data communication over ECC funded by Indian Space Research Organization data communication over ECC funded by Indian Space Research Organization

Prof. K. Viswanath Puttasandra Professor at Siddaganga Institute of Technology, Tumakur (SIT Tumkur) He obtained his Masters in signal Processing from Visvesvaraya Technological University Belgaum, India. He received Doctoral Degree in Image Transcoding and multimedia Transform domain from Indian Institute of Technology, Kharagpur. He obtained funds from various agencies.



AUTHORS PROFILE



Prof. Santhosh B received the B.E. degree in Medical electronics from Visvesvaraya Technological University Belgaum in 2005 and the MTech. Degree in Visual

Design and Implementation of Compressed Medical Data over an Authenticated Secured Channel


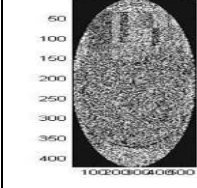

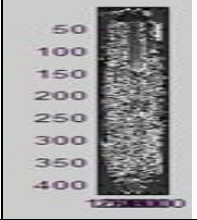

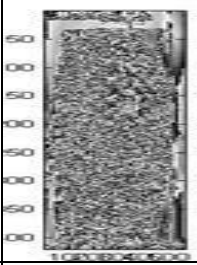

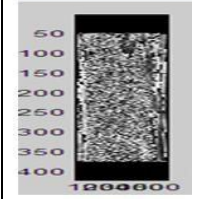

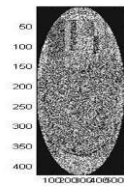
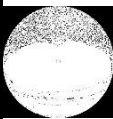
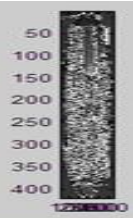
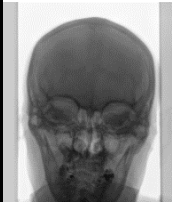
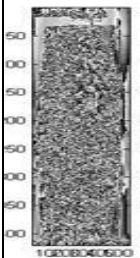

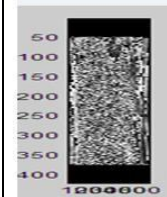
Image1	Cipher Image	Order	Public key	Private key	PSNR	MSE	NAE	SC
		4	(3,25)	(50,44)	20.5480	573.1647	0.0319	0.9793
		4	(3,25)	(50,44)	20.4992	579.6413	0.0218	0.9951
		4	(3,25)	(50,44)	19.9468	658.2675	0.0101	1.0102
		4	(3,25)	(50,44)	20.3130	605.0360	0.0133	1.0058

Image1	Cipher Image	Order	Public key	Private key	PSNR	MSE	NAE	SC
		4	(2,5)	(5,30)	20.8395	535.9519	0.0300	0.9809
		4	(2,5)	(5,30)	20.5855	568.2359	0.2124	0.9962

		4	(2,5)	(5,30)	20.0427	643.8913	.0099	1.0100
		4	(2,5)	(5,30)	20.1411	629.4565	1.0061	0.0138