Security Analysis of Medical Images using ECC over RSA

Usha Verma[1*] and Neelam Sharma[2]

[1]Banasthali Vidyapith, Tonk and MIT Academy of Engineering, Pune, India
[2]Banasthali Vidyapith, Tonk, India
[1]ushav237@gmail.com, [1]uyverma@etx.maepune.ac.in

D.O.I - 10.51201/JUSST/21/05143

http://doi.org/10.51201/JUSST/21/05143

Abstract: *The security of medical images is very important to maintain the confidentiality and privacy of patient information. Medical practitioners are required to adopt policies for the security of the access of patient's electronic information. This paper provides the security analysis of the Medical Images based on Elliptic curve cryptography. Elliptic curve cryptography (ECC) is a complex method and involves intense computation which makes it robust for the intruder attack. In this paper, ECC based Medical Image Encryption algorithm is performed on varieties of medical images like MRI, CT scan and X-ray. Security analysis is presented based on Histogram, Entropy, NPCR and UACI measures and compared with traditional method RSA. Histogram after encryption using ECC has uniform distribution which reflects that the information of original medical image is hidden properly. Entropy and NPCR achieved are 7.86 – 7.99 and 99.62 – 99.64 % respectively which are very close to their ideal values. Results reveal that ECC is more powerful and useful for medical image authentication and key distribution. However, it can be used for exchange of secret key rather than encryption.*

Keywords: Medical Image Encryption; Elliptic Curve Cryptography; NPCR; UACI; Cryptography.

1. Introduction

A drastic development in the data communication field has increased the transmission of data over internet or intranet in all the area. Hardly anyone is using traditional way of sending documents and other information manually. The same trend can be seen in the field of Medical science where patient information is gathered from the remote area and shared with the specialist doctors for diagnosis. In Medical field, the data to be transmitted is in the form of reports, images and patient personal information which may be textual. One of the core duties in medical sciences is 'Confidentiality' [18]. Ethically, patient's personal information is required to be kept private by health care providers unless the patient gives the consent to release it. Therefore, to protect patients' privacy, medical practitioners and it is required by the institutions to have policies including the security of the access of patients' electronic information.

While transmitting medical images and patient information over the network, there is a possibility of leakage as well as manipulation of information by attackers.

[*] Corresponding Author

To follow the ethical principle, it is required to adopt a robust method for the security to medical images. There are multiple techniques available to keep secret communication between sender and receiver. They are Steganography, Digital Watermarking, and Cryptography.

Steganography and Digital Watermarking are the processes where the information is hidden in the original medical image without altering its contents. Steganography is invisible and a key is having important role to retrieve the original information while watermarking can be either visible or invisible both and extraction algorithm is used to retrieve the hidden information. For medical images, mostly invisible techniques are used to hide patient's personal information [17]. Communications in Steganography are one-to-one while it is usually one-to-many in case of watermarking techniques [15]. There are various techniques of digital watermarking [8] and Steganography [5, 3].

On the other hand, Cryptography is also a technique to provide security to the images but original image is modified in such a way that it looks explicitly different from the original image and unauthorized persons could not extract any information from it [12]. This paper focuses on the security of medical images using cryptography.

More details about the Medical images and Cryptography are mentioned in section 2. Researcher's work related to medical image encryption is briefed in section 3 whereas section 4 is elaborating on ECC based medical image encryption (MIE) algorithm. Section 5 provides the implementation of medical image encryption algorithm along with security analysis. Finally work is concluded in section 6.

2. Preliminaries

2.1. Medical Images

Medical images measure physical properties of human body and made available by different modalities in the form of X-ray, MRI, CT scan, and Ultrasound images. They are interpreted by the experts of medical field like radiologist, physicians, surgeons for the purpose of taking decision for diagnosis and treatment.

Medical images are quite different from the natural images in many senses. Visual system of human being is adapted to the natural images or natural scenes but medical images are not natural one. Hence, Medical images are having such properties which differentiate them from natural images [22]. In case of natural images, the exact value of pixel intensity may typically not provide any information but it is opposite in case of Medical images. The exact value of pixel intensity in medical image provides information related to the tissue it is representing. While processing the Medical images in any term, it is required to maintain the information contained in the original image to avoid the misdiagnosis by the physicians. Accuracy plays crucial role while processing or transforming medical data.

2.2. Cryptography

The original information is coded into encrypted information using 'key' by the process *Encryption* and restoring the original information from the encrypted one is called as *Decryption*. The area of study of various encryption methods are known as *Cryptography*. The decryption methods which are not using encryption details come under the area of *Cryptanalysis*. Cryptography and Cryptanalysis are jointly termed as *Cryptology* [19].

Mainly Cryptography can be categorized in *Classical* and *Traditional* Type [19]. The taxonomy is shown in figure 1. There are two basic principles of Classical type: *Substitution* and *Transposition*. In case of *Substitution*, every element of the original data is mapped to another element whereas; in *Transposition*, elements of original data are rearranged. Caeser cipher, Playflair, Hill cipher and Vigenere cipher use Substitution principle and Rail fence cipher is the example of the Transposition principle. Traditionally, Cryptography methods are of two types: Symmetric and Asymmetric. If same key is used by sender and receiver, it is named as Symmetric or secret-key encryption. It is further divided into Block cipher and Stream Cipher. In Block cipher, blocks of input elements are processed one at a time and in Stream cipher, input elements are processed continuously. AES, DES, 3DES are the example of Block cipher whereas RC4, fish are the example of Stream cipher.

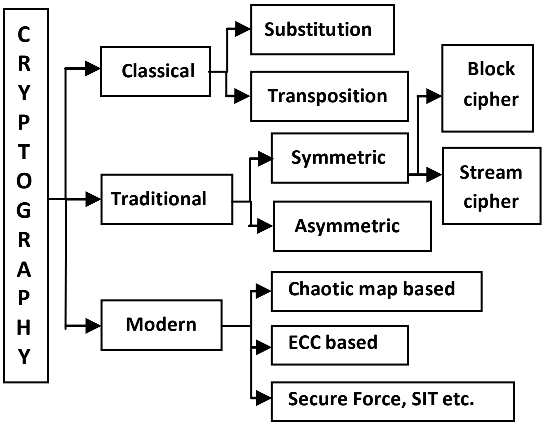


Figure.1 Classification of Cryptography

Conversely, if different keys are used by sender and receiver, then it is called as Asymmetric or public-key encryption. RSA, DSA, Deffie Hellman are the examples of Asymmetric key encryption [12].

All these classical and traditional Cryptography methods are giving satisfactory results for security of text data but they are not successful for encryption of images which contain bulk data especially medical images and satellite images [2].

Image encryption methods are not similar to data encryption methods. There are many security issues related to image processing and transmission [12]. Therefore, the other modern encryption techniques like Chaotic map based [1, 21, 7], ECC based [7, 14], Secure force algorithm [11], SIT [10] are evolved and became very popular in recent years for image encryption.

3. Related Work in Literature

The attention of researchers was drawn towards medical image encryption in the most recent years because of high need of security while transmitting medical information of patients, Medical images and reports by the physicians and care facilities to improve the communication between physicians and patients as well.

Although some work has been reported in literature in recent years in medical image encryption using various cryptography techniques but using ECC, there are few. Banu and Amirtharajan [4] have proposed an encryption algorithm for medical Images in both spatial and frequency domain by combining chaotic map with IWT and further merged with DNA sequence. They analyzed their algorithm for 50 DICOM images of size 256 x 256 and achieved an average Entropy of 7.99, key space of 10238 and NPCR, UACI values as 99.68 and 33.47 respectively.

Another work based on chaos map is presented by Han *et al.* [6] in their paper where they have used chaotic sequence to train the Hermite Choatic neural network. Analysis of results is presented using key sensitivity, histogram and key space parameters only.

A different approach of DNA cryptography is used by Akkasaligar and Biradar [13] for medical image encryption. They have proposed dual hyper chaotic map techniques along with DNA cryptography. The computational time is reduced by performing permutation and diffusion on selected pixels of medical images. The algorithm is implemented on variety of medical images like CT, MR, Ultrasound, X-ray and ECG image. Authors have claimed to achieve average Entropy of 7.85, PSNR of 5.72 and NPCR & UACI values as 99.87 & 33.29 respectively. The computational time reported is less than 0.27 sec which is good as Medical Images contain huge data. Choi *et al.* [16] presented encryption for color medical images using 3D Chaotic-Cat map and combined cellular-automata.

Chen *et al.* [20] implemented improved image encryption of medical images using high-speed scrambling and pixel adaptive diffusion. Their algorithm is based on work of Hua *et al.* [23]. First scrambling and diffusion process is carried out then insertion of some random pixels in plain image and further high-speed scrambling is performed along with pixel adaptive diffusion. Authors have claimed better results as compared to the Hua's results. Along with Entropy, histogram, NPCR, UACI and correlation, authors have presented algebraic degree analysis and chi square test to show the robustness of their algorithm against plain image attacks and brute force attack.

A comparative analysis of medical image encryption using ECC and Chaos theory is presented by Benssalah *et al.* [9]. Their results show that ECC has better performance than Choas theory but the computation time required in ECC is more. The work for medical image encryption using ECC is reported by very few researchers in the literature. Therefore it is required to work more in this area. In this paper, security analysis of ECC based Medical image encryption (ECC based MIE) is presented.

4. ECC based Medical Image Encryption (MIE) Algorithm

4.1. ECC (Elliptic Curve Cryptography)

The base of ECC is elliptic curves wherein coefficients and variables are limited to the elements of a finite field. They are actually not ellipses but as they are described by cubic equation, they are named so. The cubic equation of elliptic curves has the form of Eq.(1) which is called as 'Weierstraas equation' [19]:

$$\mathrm{y}^2 + \mathrm{axy} + \mathrm{by} = \mathrm{x}^3 + \mathrm{cx}^2 + \mathrm{dx} + \mathrm{e} \tag{1}$$

This equation is limited to the Eq. (2) for the purpose of understanding ECC:

$$y^2 = x^3 + \mathrm{a}x + \mathrm{b} \tag{2}$$

where a, b are real numbers and x, y take the values in the real numbers. To plot elliptic curve from this equation, it is required to compute *y* using Eq.(3).

$$y = \sqrt{x^3 + ax + b} \tag{3}$$

For the given values of *a* and *b*, *y* has both positive and negative values for every x value. Such elliptic curve is shown in figure 2 depicting the set E(1,1) respectively. Curve is symmetric about x-axis i.e. *y=0*. E(*a*,*b*) consist of all points (*x*,*y*) which satisfy Eq. (1) with the *O* element.

Addition Rule:
Addition operation is defined for E(*a*,*b*) and the Eq. (4) is satisfied by *a* and *b:*

$$4a^3 + 27b^2 \neq 0 \tag{4}$$

Geometrically, rule of addition is: When three points of an elliptic curve are on a straight line, the sum of these three points is *O* (*zero point* or *point at* infinity).

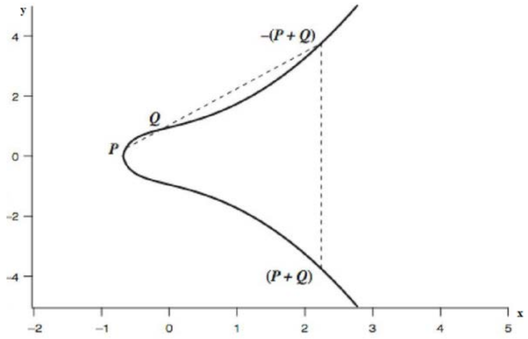


Figure 2. Elliptic curve of set E(1,1) with $y^2=x^3+x+1$

O= -O; for P which is a point on the elliptic curve, P + O = P by assuming P ≠ O & Q ≠ O. If P = (x,y), then its negative point is –P = (x,-y) and these two points P and –P can be connected through a vertical line. The addition of these two points is: P + (-P) = P – P = O.

Now consider P and Q; two points with different x coordinates. While connecting these two points with a straight line; a third point of intersection (R) is obtained. Now the addition on these three points is defined such that P + Q to be the mirror image of R w.r.t. x axis → P + Q = - R.

For cryptographic applications, two types of elliptic curves are used: Binary curves over GF (2^m) and Prime curves over Z_p. For hardware applications, binary curves are best whereas prime curves are best for software applications [19].

ECC is a space optimized encryption algorithm which provides more security with smaller key size as its foundation is DLP (Discrete Logarithm Problem). Due to its complexity, it became a strong encryption method to secure against the attacks but require more computational time comparative to other image encryption methods [7].

4.2 Algorithm

The complete flow of the Medical Image Encryption (MIE) using ECC is shown in the figure 3. It has mainly four blocks: Global parameters selection, Key generation and Exchange, Encryption and Decryption. The step by step algorithm is explained further:

Global parameters:
(1) Select q; a large integer which is a nothing but a prime number ‘p’.
(2) Select a and *b* parameters of elliptic curve equation.
(3) Define Eq (a,b).
(4) Select base point G=(x1, y1) of order ‘n’ in Eq(a,b).
(5) The ‘n’ is smallest +ve integer which satisfies nG=0.

Key Generation and exchange:
(6) Sender select private key ns < n.
(7) Public key Ps = ns x G is generated by sender; which is also a point on Eq(a,b).
(8) Receiver also select private key nr < n.
(9) Receiver generates public key Pr = nr x G.
(10) Sender and receiver share their public key on secure media.

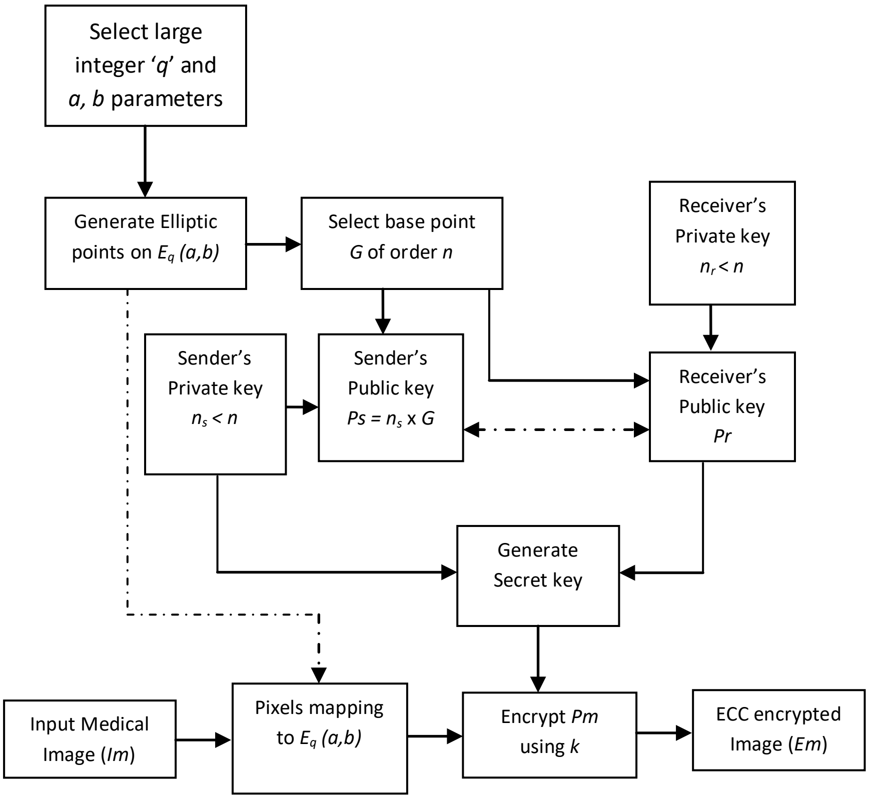

Select large integer ‘q’ and a, b parameters
Generate Elliptic points on E_q (a,b)
Select base point G of order n
Receiver’s Private key $n_r < n$
Sender’s Private key $n_s < n$
Sender’s Public key $Ps = n_s$ x G
Receiver’s Public key Pr
Generate Secret key
Input Medical Image (Im)
Pixels mapping to E_q (a,b)
Encrypt Pm using k
ECC encrypted Image (Em)

Figure 3. ECC based Medical Image Encryption (MIE)

Encryption:

(11) Take the original medical image Im of size M x N.

(12) Map the pixels of the medical image to the Elliptic curve points, Eq(a,b) and get matrix Pm.

(13) Apply receiver's public key to generate the secrete key k = ns x Pr.

(14) Encrypt Pm using k to get Encrypted image matrix (Em):
Em = {kG, (Pm+kPr)} = {E1, E2}.

Decryption:

(15) Encrypted image is received by receiver having two components E1 and E2.

(16) Receiver multiplies E1 with own private key nr = nr(kG).

(17) Then subtracts from E2 to get Pm:
(Pm+kPr)- nr(kG)= Pm+k nrG - nrkG= Pm

(18) Original medical image is retrieved by inverse mapping.

5. Implementation and Security Analysis

5.1. Implementation

The simulation is performed on a laptop having processor Intel(R) Core(TM) i3-5005U CPU @ 2.00 GHz (4CPUs), 4GB RAM and Windows 10 operating system using MATLAB R2018b. The medical images used are taken from internet for the sole purpose of study and research. Various types of medical images like MRI, CT scan and X-ray, are encrypted using ECC. In figure 4, the encrypted and decrypted images are shown along with the original medical images.

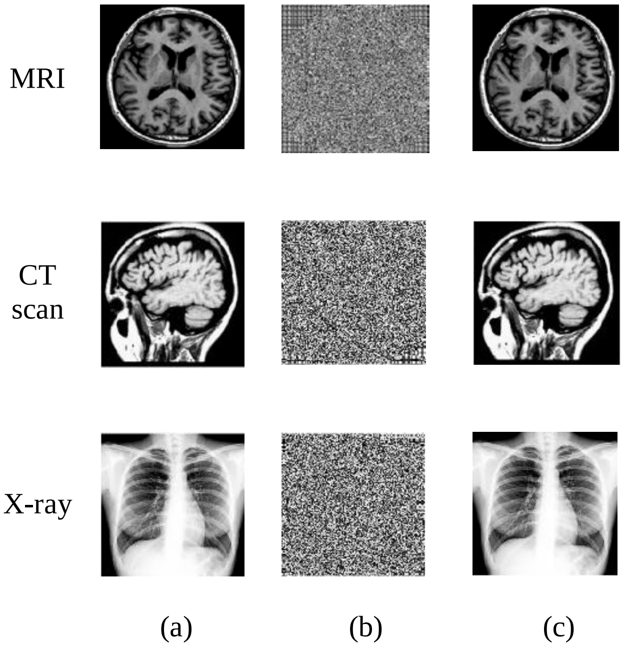


Figure 4. ECC based Encryption and Decryption (a) Original Medical Image (b) Encrypted Medical Image (c) Decrypted Medical Image

It is clear that the ECC based Medical Image Encryption (MIE) algorithm transforms the original image into encrypted images with random distribution and it is hard to obtain original medical image from the encrypted medical image by the attackers. The security analysis presented in the next sub-section justifies this.

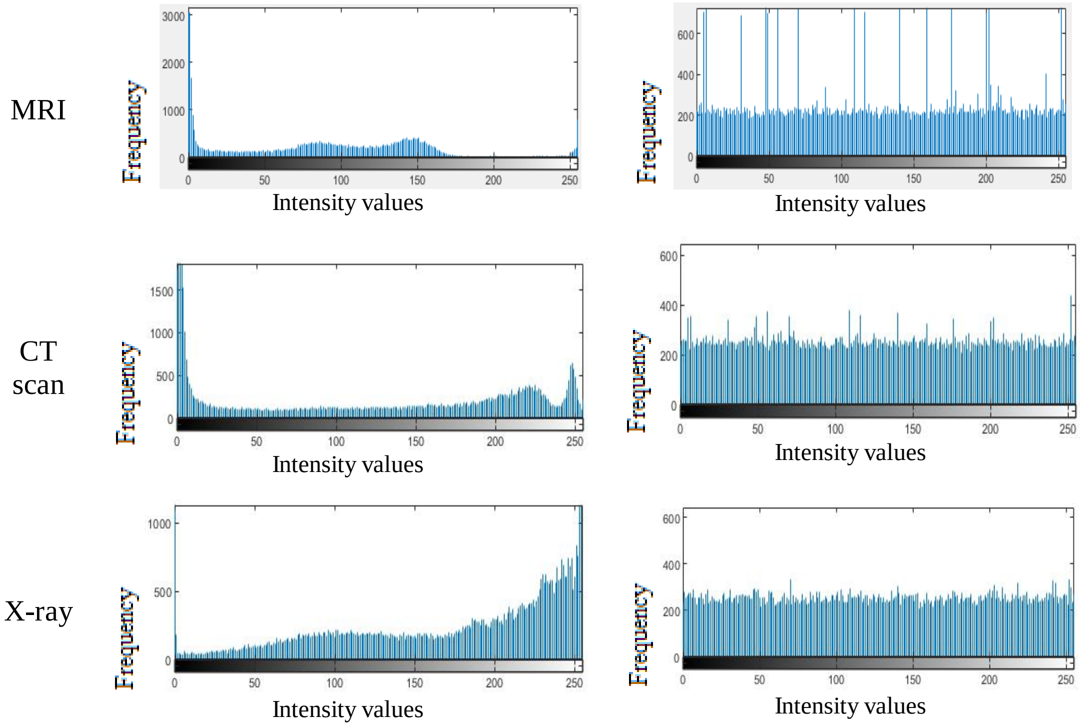
5.2. Security Analysis

5.2.1. Histogram Analysis

The discrete function of the histogram of a gray scale digital image with L intensity values in the range [0, L-1], represented by Eq. (5):

$$H(r_k) = n_k \tag{5}$$

where n_k represents count of pixels in a digital image with pixel intensity (rk) [20].



(a) Histogram of original image (b) Histogram of encrypted image

Figure 5. Histogram Analysis (a) Original image (b) Encrypted image

It gives a visual representation of the pixel distribution. By looking at it, a viewer can judge about the image and can retrieve information using some algorithm. For a robust encryption algorithm, encrypted medical image is having uniform distribution in histogram to reflect that the information of original medical image is hidden properly.

Figure 5 shows the histogram of the original medical images as well as their encrypted medical images. It is observed that histogram of original medical images are varying a lot whereas histograms of their encrypted images are evenly distributed. It indicates goodness of encryption method and therefore attackers will not find any useful information from the encrypted images.

5.2.2. Entropy Analysis

Entropy gives average information of an image. It is a measure of degree of uncertainty or randomness in the image. For a digital image having L intensity values in the range [0, L-1], it is given by the Eq. (6) [20]:

$$H(k) = -\sum_{i=0}^{L-1} P(k_i)\, log_2 P(k_i) \qquad (6)$$

where, $P(k_i)$ is the occurrence probability of the i^{th} symbol k_i.

For an entirely random image where the occurrence probability of every pixel intensity is equal; can be easily calculated. Like, for an image with L=256, entropy should be 8 ideally. An encrypted image should have the high degree of randomness or uncertainty so that attackers could not retrieve information from it. The medical images here considered are gray scale image with L=256.

Table 1. Comparative Analysis of ECC based MIE and RSA

Method	Image Type	Entropy		NPCR (%)	UACI (%)
		Original Image	Encrypted Image		
ECC based MIE	MRI	5.9978	7.8641	99.64	31.28
	CT scan	6.8252	7.9910	99.62	25.52
	X-ray	7.3761	7.9954	99.63	11.62
RSA	MRI	5.9978	7.3844	99.64	28.73
	CT scan	6.8252	7.8341	99.59	24.32
	X-ray	7.3761	6.6693	99.64	8.62

Table 1 shows the entropy values of original medical images and their encrypted images as well for ECC based MIE and compared with RSA. It can be noticed that entropy values of encrypted images using ECC based MIE are in the range from 7.86 to 7.99 which are almost equal to 8. It points toward the better randomness than that of RSA which is also represented in figure 6.

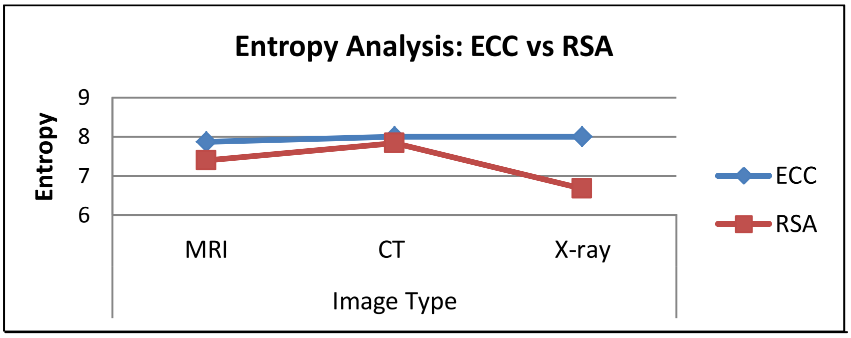


Figure 6. Entropy Analysis of ECC based MIE and RSA

5.2.3. NPCR and UACI measure

A good image encryption algorithm should withstand chosen-plaintext attack. The encrypted image of original image should be completely different even if a single bit is changed in original one. The sensitivity can be measured by two indices: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity), which are defined by Eq. (7) and (8) respectively.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\ \% \tag{7}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255}\right] \times 100\ \% \tag{8}$$

where, M x N is size of encrypted image. E1(i,j) is the encrypted image of original image and E2(i,j) is the encrypted image after the single bit is changed in the original one. D(i,j) is the difference array calculated by Eq. (9).

$$D(i,j) = \begin{cases} 1, & \text{if } E_1(i,j) \neq E_2(i,j) \\ 0, & \text{if } E_1(i,j) = E_2(i,j) \end{cases} \tag{9}$$

The ideal values of the two measures; NPCR & UACI for digital images with L=256 are 99.6094% and 33.4635% respectively [20]. If values of NPCR and UACI of encryption algorithm are close to ideal values then it is a sign of robust encryption to withstand the differential attacks. It can be observed from the figure 7 and table 1 that for medical images with L=256, the NPCR values are very close to ideal values for ECC based MIE as compared to RSA. Whereas, UACI values are slightly deviating from the ideal values for some of medical images but giving better results in case of ECC based MIE than RSA.

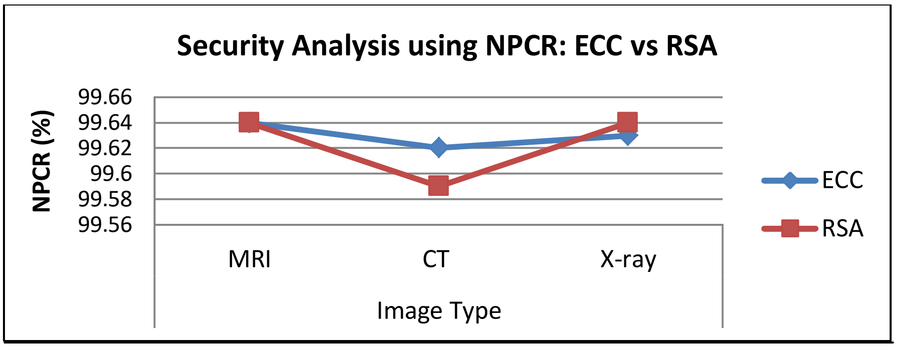


Figure 7. Security Analysis using NPCR for ECC based MIE and RSA

6. Conclusion

ECC is an Asymmetric Encryption method which proves security of Medical images. The Histogram analysis and Entropy analysis using ECC based MIE presented in this paper reveals that all types of medical images like MRI, CT Scan and X-ray, are perfectly encrypted and have sufficient randomness. NPCR values are very close to ideal values but the slight deviation of UACI values in few cases. When compared with traditional RSA encryption method, ECC based MIE is providing better results.

For the security of Medical images and authentication of patient's information, it is required to send the patient's personal information along with the digital medical images. For that purpose, the hybrid method using watermarking and cryptography can be evolved. We conclude by raising research issues and suggestions to integrate digital watermarking and cryptography to produce a robust hybrid technique for authentication and security of medical images and patient's information both. In such hybrid methods, ECC can play important role for key exchange.

Acknowledgments

The implementation of this work is facilitated by MIT Academy of Engineering; therefore authors show thankfulness to the institute. Authors are also grateful to the AIM & ACT, Banasthali Vidyapith for giving opportunity to do work on the topic.

References

[1] *A. Arab, M. J. Rostami and B. Ghavami, "An image encryption method based on chaos system and AES algorithm", The Journal of Supercomputing, Vol. 75, (2019) pp. 6663–6682.*

[2] *A. M. Ghaleb, S. Sasi and A. R. Aswatha, "Design and Implementation of Satellite Image Encryption by using ECC", 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology, Bengaluru, (2018), pp. 1438-144.*

[3] *A. S. Ansari, M. S. Mohammadi and M. T. Parvez, "Comparative Study of Recent Steganography Techniques for Multiple Image Formats", International Journal of Computer Network and Information Security, Vol. 1, (2019), pp. 11-15.*

[4] *A. S. Banu and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach", Medical & Biological Engineering & Computing, Vol. 58, No. 7, (2020), pp. 1445-1458.*

[5] *A. Sharma, R. K. Buraniya and P. K, "Steganography: An Overview", International Journal for Technological Research in Engineering, Vol. 6, No. 7, (2019), pp. 5084-5086.*

[6] *B. Han, Y. Jia, G. Huang and L. Cai, "A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network", IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, Chongqing, (2020), pp. 2644-2648.*

[7] *C. R. Revanna and C. Keshavamurthy, "Hybrid Method of Document Image Encryption using ECC and Multiple Chaotic Maps", International Journal of Recent Technology and Engineering, Vol. 8, No. 4, (2019), pp. 1615-1629.*

[8] *J. S. Gaikwad and U. Verma, "Digital Image Watermarking by Fusion of Wavelet and Curvelet Transform", Advances in Signal and Data Processing. Lecture Notes in Electrical Engineering, Springer, Singapore, Vol. 703, (2021), pp. 545-559.*

[9] *M. Benssalah, Y. Rhaskali and M. S. Azzaz, "Medical Images Encryption Based on Elliptic Curve Cryptography and Chaos Theory", IEEE, (2018), pp. 222-226.*

[10] *M. Usman, I. Ahmed, M. I. Aslam, S. Khan and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, (2017), pp. 402-411.*

[11] *M. V. Babu, M. N. Kalyan, K. Amjesh, M. S. Krishna and J. R. Teja, "A Secure Image Transmission using Secure Force Low Complexity Encryption Algorithm with Histogram Analysis", Anveshana's International Journal of Research in Engineering and Applied Sciences, Vol. 3, No. 4, (2018), pp. 37-39.*

[12] *O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree and F. Y. H. Ahmed, "A Survey and Analysis of the Image Encryption Methods", International Journal of Applied Engineering Research, Vol. 12, No. 23,(2017), pp. 13265-13280.*

[13] *P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography", Information Security Journal: A Global Perspective, Vol. 29, No. 2, (2020), pp. 91-101.*

[14] *S. Bendaoud, F. Amounas, E. Hassan and E. Kinani, "An Enhanced Image Encryption Scheme Based on ECC and PWLCM", International Journal of Scientific Research in Science, Engineering and Technology, Vol. 6, No. 4,(2019), pp. 285-293.*

[15] *S. K. Dubey and V. Chandra, "Steganography, Cryptography and Watermarking: A Review", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, No. 2, (2017), pp. 2595-2599.*

[16] *U. S. Choi, S. J. Cho and S. W. Kang (2020), "New Color Encryption for Medical Images Based on Three Dimensional Generalized Chaotic Cat Map and Combined Cellular Automata", Advances in Science, Technology and Engineering Systems Journal, Vol. 5, No. 2, (2020), pp. 104-110.*

[17] *U. Verma and N. Sharma, "Hybrid Mode of Medical Image Watermarking to Enhance Robustness and Imperceptibility", International Journal of Innovative Technology and Exploring Engineering, Vol. 9, No. 1,(2019), pp. 351-359.*

[18] *UW Medicine, Department of Bioethics and Humanities, "Bioethics Topics" [Online]. Available: https://depts.washington.edu/bhdept/ethics-medicine/bioethics-topics. [Accessed 30-Dec-2020]*

[19] *W. Stallings, Cryptography and Network Security: Principles and Practices, 7th ed. Pearson Education, India, (2018).*

[20] *Y. Chen, C. Tang and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Processing Journal, Vol. 167, (2019), pp. 1-12.*

[21] *Y. Luo, X. Ouyang and J. Liu, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems", IEEE Access, Vol. 7, (2019), pp. 38507-38522.*

[22] *Y. Xu, A. Raj and J. D. Victor, "Systematic Differences between Perceptually Relevant Image Statistics of Brain MRI and Natural Images", Front. Neuroinform., Vol. 13, No. 46, (2019), doi: 10.3389/fninf.2019.00046.*

[23] *Z. Hua, S. Yi and Y. Zhou, "Medical Image Encryption using high-speed scrambling and pixel adaptive diffusion", Signal Process, Vol. 144, (2018), pp. 134-144.*