Implementation of Image Encryption Using Elliptic Curve Cryptography

J. Ravi[1] , K. VenkatRao[2]. N. Kishore Chandra Dev[3], M. Praveen Kumar[4]

[1234]*Assistant Professor, ECE Department*

[1234]*SRKR Engineering College, Bhimavaram*

Abstract - This Paper represents an approach to implement image encryption scheme. Encryption can provide a means of securing information and message authentication. This project presents a new effective technique based on elliptic curves for securing images over public channels. Cryptography is a solution to protect confidential images by encrypting them before transmission over unsecure channels or public networks. In recent years, elliptic curve cryptography (ECC) has gained widespread exposure and acceptance, and has already been included in many security standards. The idea of Elliptic Curve Cryptography (ECC), and how it has a better promise for a faster and more secure method of encryption in comparison to the currents standard in the public key cryptographic algorithms. The ECC covers all relevant asymmetric cryptographic primitives like digital signatures and key agreement algorithms.ECC uses smaller keys to provide high security and high speed. Elliptic Curve Cryptography (ECC) is based on computational operations (Add, Double, Multiply) on the points that lie on a predefined elliptic curve. This cryptosystem also utilize a new mapping method to convert to convert every pixel of plain image into a point on an elliptic curve, which is a mandatory prerequisite for any ECC based encryption. Encryption and decryption process are given in detail with implementation. After applying encryption process, security analysis is performed to evaluate the strength of the proposed technique to statistical attacks.

Keywords: Image Encryption, Decryption, Elliptic Curve Cryptography

I. INTRODUCTION

Multimedia refers to content that uses a combination of different content forms. This contrasts with media that uses only rudimentary computer displays such as text only or traditional forms of printed or hand-produced material. Multimedia includes a combination of text, audio, still images, animation, video or interactivity content forms. Multimedia is usually recorded and played, displayed, or accessed by information content processing devices, such as computerized and electronic devices, but can also be part of a live performance. Multimedia devices are electronic media devices used to store and experience multimedia content. Multimedia is distinguished from mixed media in fine art; by including audio, for example, it has a broader scope. The term “rich media” is synonymous for interactive multimedia. Hypermedia can be considered one particular multimedia application.

II. IMAGE REPRESENTATION

An image is stored as a matrix using matlab matrix conventions. Here are three basic types of images.

1.Binary image 2.Gray scale image 3.RGB image

III. ENCRYPTION

The word “encryption” has been coined from the word “cryptography” which is derived from the Greek “kryptos” (hidden) and “graphics” (writing). Encryption is the process of transforming text into an unintelligible form called cipher. Data encryption is the process used to hide the true meaning of data.

Reversing the process of encryption is called decryption. Encryption and decryption comprise the science of cryptography as it is applied to the modern computer. Data encryption is achieved through the use of an algorithm that transforms data from its intelligible form to cipher. An algorithm is a set of rules or steps for performing a desired operation. An algorithm can be performed by anything that can be taught or programmed to follow a specific and unambiguous set of instructions.

IV. CONCEPTS OF IMAGE ENCRYPTION

Image encryption is necessary for future multimedia internet applications. Password codes to identify individual users will likely be replaced are biometric images of fingerprints and retinal scan in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper may duplicate or reroute the information. By encrypting these images, a degree of security can be achieved. Furthermore, by encrypting non-critical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information.

Image encryption can also be used to protect privacy. An example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the cost and to improve service, electronic forms of medical records have been sent over networks from laboratories to medical centers. According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks. Unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps, which are deterministic but simple. Chaotic maps present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security. Therefore, it can provide a fast and secure means for data protection, which is crucial for image data transmission over fast communication channels, such as the broadband internet communication.

The main obstacle in designing image encryption algorithm is that it is rather difficult to swiftly confuse and diffuse data by traditional means of cryptology. In this respect, chaos-based ciphers have shown their superior performance. It has been proved that in many aspects those chaotic maps have been analogous but different characteristics as compared with conventional encryption algorithm.

V. APPLICATIONS OF VARIOUS TYPES OF ENCRYPTION

Symmetric encryption works well when encoding personal data and data stored inside a secure system where outsider cannot access it. If you have to sent a data using insecure method such as email, outsider may be able to intercept the key, giving them access to all communications. An asymmetric system would work best in that case, since even if they captured a public key, it would be no good for decryption. Password and other security systems can make use of hashing techniques, since the system can store hashed passwords in a database and hash a user's input to compare the values. Even if outsiders manage to steal the hashed passwords, they have no way to decode the encrypted passwords into their readable form.

VI. ELLIPTIC CURVE CRYPTOGRAPHY

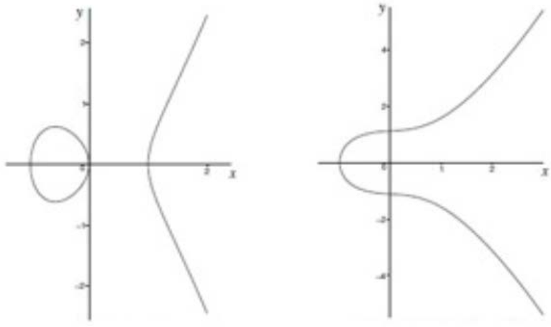
Elliptic Curve Cryptography is a public key cryptography. It is based on elliptic curves. It was proposed independently by Neal Koblitz and Victor Miller in 1985. While solving for arc length of an ellipse, elliptic curve equation was found. Elliptic Curve is defined by the following Weierstrass Equation.

$Y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ Eq. 1: Weierstrass equation

An elliptic curve is defined over real numbers. Elliptic curve is defined by set of points of a curve equation above.

$Y^2=x^3+ax+b$, where $4a^3+27b^2\neq0$ Eq. 2: Elliptic Curve Equation

To satisfy non-singularity without cusps or self-intersections on the elliptic curve the condition to be met is $4a^3+27b^2\neq0$. A sample of elliptic curves is shown in figure 1. In ECC, a private key and the corresponding public key is a point on the EC and this public key is known to all the users who are in communication range. The Encryption and decryption operations are performed on the curve points. Elliptic curves for Cryptographic application are defined over prime field and binary field.



1. $y^2=x^3-x$ and 2. $Y^2=x^3+1/4x+5/4$

Figure 1. Example of elliptic curves over Real Field

Elliptic Curve Cryptography (ECC) is an emerging PKC algorithm. Wang Wei-Hong, Lin Yu-Bing and Chen Tie-Ming proposed study and application of ECC in WSN, explains Tiny OS Developing Environment, and basics of ECC over prime field and its expressions to implement in software level, expresses the comparison of ECC over RSA/DSA based on key sizes. ECC is able to replace the RSA algorithm in the near future. ECC requires lesser key size compared to RSA for the equal amount of security. Monsef Amara and Amar Siad discussed the comparison of ECC over RSA, give brief explanation of ECC and mathematical operations of Elliptic Curve Cryptography and revealed various methods to implement scalar multiplication.

VII. EXPERIMENTAL RESULTS

SECURITY ANALYSIS:

To test our proposed encryption method, several experiments were performed. The proposed algorithm is implemented and analyzed by MATLAB programming language on a PC with Intel Core i3 2.3 GHz CPU, 8 GB of RAM and a 32-bit OS.

The mapping results are shown below. Since each value corresponding to a pixel lies in integral range of 0 to 255, we needed a minimum of 256 points on the curve. So after doing a lot of trials using various prime numbers (p), finally landed at a value of p307. And the parameters of the curve are chosen to be a=-3 and b=3 and following the procedure of comparison of the RHS and LHS values by evaluating them through the prime field operations we obtained 285 points on the Elliptic curve chosen for the parameters assumed.

Some of the points on the Elliptic curve are as follows:

(1,1),(1,306),(5,128),(5,179),(6,87),(6,220),(8,106),(8,201),(12,62),(12,245),(16,47),(16,260),(17,80),(17,227),(18,116),(18,191),(27,112),(27,195),(31,42),(31,265),(32,146),(32,161),(33,42),(33,265),(34,38),(34,269),(35,10),(35,297),(38,27),(38,280),(42,63),(42,244),(43,92),(43,215),(44,4),(44,303),(45,11),(45,296),(51,106),(51,201),(52,69),(52,238),(53,146),(53,161),(54,11),(54,296),(59,71),(59,236),(61,34),(61,273),(66,16),(66,291),(68,28),(68,279),(69,95),(69,212),(70,117),(70,190),(71,53),(71,254),(77,32),(77,275),(78,96),(78,211),(79,101),(79,206),(82,47),(82,260),(84,49),(84,258),(86,2),(86,305),(87,61),(87,246),(88,63),(88,244),(90,23),(90,284),(92,28),(92,279),(94,22),(94,285),(95,16),(95,291),(101,4),(101,303),(103,27),(103,280),(106,48),(106,259),(107,114),(107,193),(108,153),(108,154),(109,123),(109,184),(110,83),(110,224),(112,101),(112,206),(113,215),(113,182),(115,24),(115,283)etc.

These points will be mapped to the range of pixel values in case of images and the process of encryption and decryption are as usual.

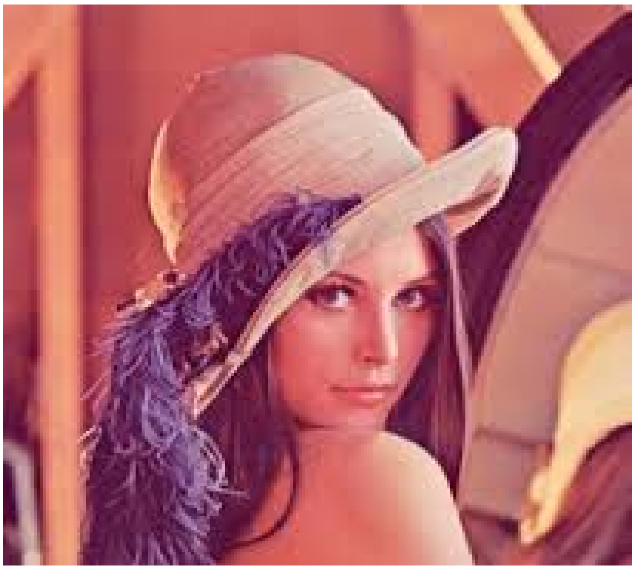


Fig2.1(a)Lena Image

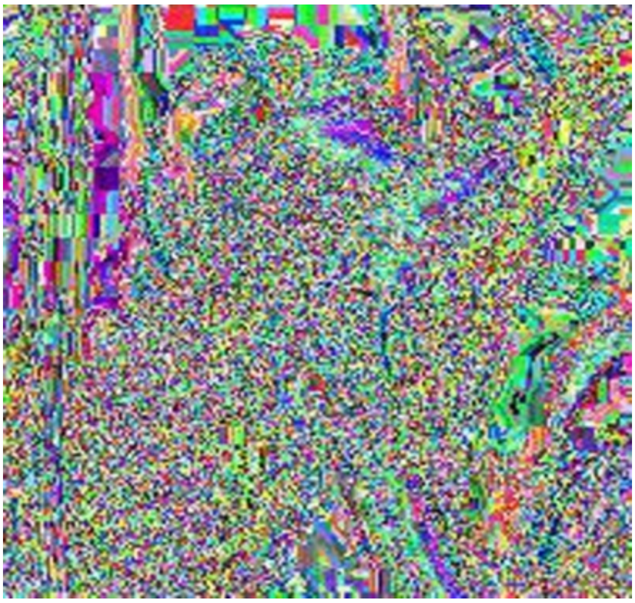


Fig2.1(b)Encrypted Image

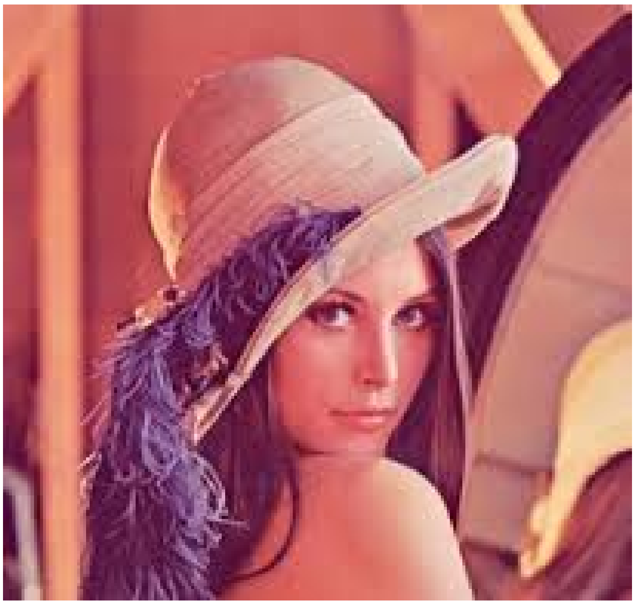


Fig 2.1(c) Ideal Decrypted Image

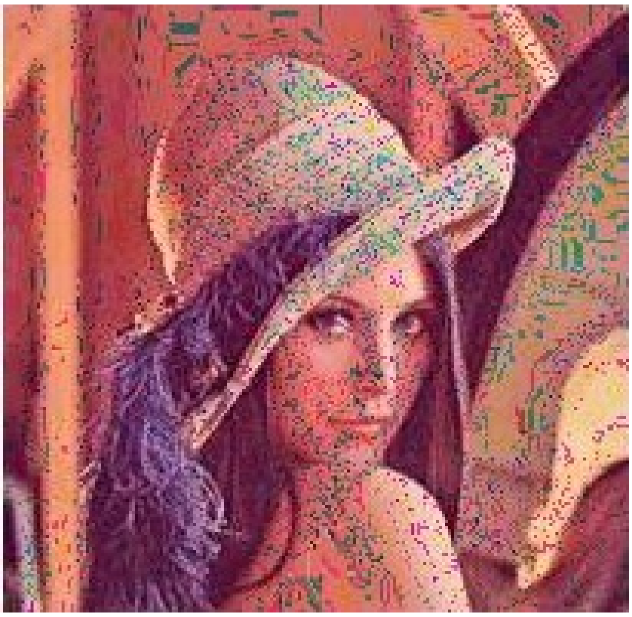


Fig 2.1(d) Practical Decrypted image

Table 1. Estimated running times

Image	Mapping Time(Sec)	Encryption Time(Sec)	Decryption Time(Sec)
Lena Image	0.05	8.46	8.21
Logo Image	0.04	8.01	7.20

VIII. CONCLUSION

Elliptic Curve Cryptography is an almost new public key cryptosystem, and provides equivalent security with a smaller key size, low mathematical complexity, and is computationally more efficient than RSA. High-speed encryption and saving bandwidth, makes ECC an acceptable option for high data rate and real time applications, such as image and multimedia encryption. Encryption and decryption is based on points. A plain message should be converted to a point and the results of encryption are also points. Hence all the operations are based on the points on the elliptic curves. In this study, a new mapping method was introduced to convert a pixel's value to a point on an affine elliptic curve over a finite field *GF(p)* using a map table. This mapping technique is fast, has low complexity and computation, is easy to implement, and has similar performance on images with low diversity in grey levels. Security analysis on encrypted images proved the strength of the proposed scheme and its robustness to statistical attacks. Elliptic curve cryptography with the proposed modifications namely Dynamic generator and Gyrator mapping are very much helpful in successful encryption and decryption.

IX. FUTURE SCOPE

1.For future work, this method could be combined with a chaos map to achieve hybrid cryptography to more diffusion and confusion, with respect to running time efficiency and expanding key space.

2. There is a need to establish a way such that this algorithm can be applied over delay intolerant multimedia data types i.e. video conferencing and video calling.

3.Choice of algorithms which consumes less time in software implementation such as heap search instead of binary search we need for searching inverse of a number or point from mapping.

REFERENCES

[1] V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology, Springer-Verlag vol.85, pp. 417-426, 1986.

[2] N. Koblitz, "Elliptic curve cryptosystems", Mathemathics of Computation, AMS, vol. 48, no.177,pp. 203-208, 1987.

[3] G. Zhu, W. Wang, X. Zhang and M. Wang, "Digital image encryption algorithm based on pixels", Proceedings of the IEEE International Conference on Intelligent Computing and Intelligent Systems (CIS' 10), China, pp. 769-772, 2010.

[4] K. Gupta and S. Silakari, "Efficient hybrid image cryptosystem using ECC and chaotic map",International Journal of Computer Applications, FCS, vol. 29, no. 3, 2011.

[5] K. Gupta, S. Silakari, R. Gupta and S.A. Khan, "An ethical way for image encryption using ECC", Proceedings of the 1st International Conference on Computational Intelligence, Communication Systems and Networks, 2009.

[6] B. Padma, D. Chandravathi and P. Roja, "Encoding and decoding of a message in the implementation of elliptic curve cryptography using koblitz's method", Int. J. Comput. Sci. Eng., vol. 2, no. 5, pp. 1904-1907, 2010.

[7] F. Amounas and E.H.E. Kinani, "Fast mapping method based on matrix approach for elliptic curve cryptography", Int. J. Inform. Netw. Sec., vol.1, no.2, pp. 54-59, 2012.

[8] F. Amounas and E.H.E. Kinani, "An efficient elliptic curve cryptography protocol based on matrices", Int. J. Eng. Invent., vol.1, no.9, pp. 49-54, 2012.

[9] O.S. Rao and S.P. Setty, "Efficient mapping method for elliptic curve cryptosystems", Int. J. Eng.Sci. Tech., vol. 2, pp. 3651-3656, 2010.

[10] S. Gupta, P.S. Gill, A. Mishra and A. Dwivedi, "A scheme for secure image transmission using ECC over the fraudulence network", International Journal Adv. Res. Comput. Sci. Soft. Eng., vol.2, no.4, pp. 67-70, 2012.

[11] A. Soleymani, Zulkarnain Md Ali, M. J. Nordin, "A Survey on Principal Aspects of Secure Image Transmission", World Academy of Science, Eng. and Technology, vol. 66, pp. 247-254, 2012.

[12] Certicom, "Certicom ECC Challenge", Certicom Research, 2009.

[13] C.S. Yeh, I.S. Reed and T.K. Troung, "Systolic multipliers for finite fields GF(2m)", IEEE Trans. Computers, C-33, pp: 357–360, 1984.

[14] M.Antonini, M.Barlaud, P.Mathieu, and I.Daubechies, Image Coding Using the Wavelet Transform, *IEEE Trans on Image Processing*, 2(2), Pages 205-220, 1992.

[15] K. Kinebuchi, D. D. Muresan, and R. G. Baraniuk, "Wavelet based statistical signal processing using hidden Markov models," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, vol. 3, pp. 7–11, 2009.

[16] J.Núñez, X.Otazu, O.Fors, A.Prades, V.Palà, and R.Arbiol, Multi resolution-Based Image encryption with Additive Wavelet Decomposition, *IEEE Transactions on Geo science and Remote Sensing*, vol.27, no. 3, Pages. 1305-1311, 1999.

[17] H. Demirel and G. Anbarjafari, " image encryption using elliptic curve cryptography," *IEEE Geoscience and Remote Sensing Letter*, vol. 5, no. 2, pp. 133–136, 1998.

[18] Y. Piao, I. Shin, and H. W. Park, "Image resolution enhancement using inter-sub band correlation in wavelet domain," in *Proc. Int. Conf. Image Process.*, vol. 1, pp. I-445–448, 2007.

[19] Y. Rener, J. Wei, and C. Ken, "Down sample-based multiple description coding and post-processing of decoding," in *Proc. 27th Chinese Control Conf.*, Jul. 16–18, pp. 253–256, 2008.

[20] C. B. Atkins, C. A.Bouman, and J. P. Allebach, "Optimal image scaling using pixel classification," in *Proc. Int. Conf. Image Process.*, Oct. 7–10, vol. 3, pp. 864–867, 2001.