ISSN 2349-0292
Impact Factor 3.802

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

ELLIPTIC CURVE CRYPTOGRAPHY AND ARNOLD CAT MAP ON BIOMETRIC IMAGES

D.M.S. Bandara[(1)] , E.M.C.L. Ekanayake[(2)]
[(1)] Wayamba University of Sri Lanka.
[(2)] Wayamba University of Sri Lanka.

DOI: 10.5281/zenodo.2449397

ABSTRACT

Biometric images are detailed, unique, difficult to alter and durable over the life of an individual, making them suitable as long-term markers of human identity. In recent years cryptographic algorithms have been suggested to secure biometric images. In this paper, mainly consider on fingerprint images and we propose a new algorithm to encrypt and decrypt fingerprint images by using a specially designed Elliptic Curve Cryptography (ECC) procedure. In addition, to increase the confuseing effect of fingerprint encryption, we also utilize Arnold Cat Map (ACM) for a shuffling of pixel locations in our method. Moreover, we use block ciphers for reducing the computational space and time. Experimental results are carried out with detailed analysis to demonstrate that the proposed encryption-decryption algorithm is advantageous in several different aspects including efficiency, security and flexibility.

KEYWORDS: Image Encryption, Biometric Encryption, Fingerprint image, Elliptic Curve Cryptography, Arnold Cat Map, Koblitz's Encoding, Encryption and Decryption.

INTRODUCTION

A biometric is defined as a unique, measurable, biological characteristic or quality for automatic identification and verification of the identity of a human being. Analyzing of these biological characteristics has become known as the science of biometrics. These days, biometric technologies are usually used to analyze human characteristics for security purposes.

The exchange of these biometric data over unsecured network channels makes it at risk to the violation of security by illegal accesses. To overcome this challenge, in this paper we propose an efficient and secure encryption scheme which behaves with remarkable complexity and is difficult to predict and hack for intruders.

Combining biometrics and cryptography has the potential to provide higher assurance of system security. A security scheme that utilizes both biometrics and crypto keys is known as biometric encryption. In this paper, we use fingerprint images as biometric data. Moreover, the cryptographic technique which we have used in this paper is specialized design based on block ciphers and the general Elliptic Curve Cryptography (ECC) which is a public key cryptosystem originally developed by Neal Koblitz and Victor S. Miller in 1985 [1][2]. After 2004 ECC becomes widely used for information security as an encryption tool.. Many researchers have concluded that the difficulty of solving of Elliptic Curve Discrete Logarithmic Problem over finite fields is very hard with respect to a proper key size and this property enables ECC to be remarkable tool for encryption and decryption processes under various circumstances. In particular, for this research, we use three different prime fields with respect to three different bit sizes of 128, 256 and 512 bits as the underlying finite fields of ECC. Fingerprints are encrypted on using ECC over these three prime fields. Furthermore, for increasing the overall performance of our method, we also incorporate Arnold's Cat Map (ACM) for permuting pixel locations as an initial step of encrypting the fingerprint images.

MATHEMATICAL PRELIMINARIES

The most important mathematical operations regarding ECC are briefly explained in the following.

An elliptic curve over a prime number p is an algebraic group defined by a cubic equation with the form $Y^2=\{x^3+ax+b\}$ mod p where $4a^3+27b^2\neq 0$.

Point addition, subtraction, multiplication and doubling are the key arithmetic operations on an elliptic curve.

ISSN 2349-0292
Impact Factor 3.802

A. Point Addition

Point R with coordinates (x_3,y_3) is a sum of Point P (x_1,y_1) and Point Q (x_2,y_2) under the group addition of the elliptic curve.

$P(x_1,y_1) + Q(x_2,y_2) = R(x_3,y_3)$

$x_3=(k^2-x_1-x_2) \bmod p$, $y_3=(k(x_1-x_3)-y_1) \bmod p$

where $k=(y_2-y_1) / (x_2-x_1) \bmod p$

B. Point substraction

For subtraction, we mirror the coordinates of particular point along the x-axis and apply the above addition operation to compute subtraction as follows

$P(x_1,y_1) - Q(x_2,y_2) = P(x_1,y_1) + Q(x_2,- y_2)$.

C. Point doubling

To compute point doubling, we identify point P and point Q in the point addition formula

$P(x_1,y_1) + Q(x_1,y_1) = R(x_3,y_3)$

$x_3=(k^2-2x_1) \bmod p$, $y_3=(k(x_1-x_3)-y_1) \bmod p$

where $k=(3x_1^2 + a) / 2y_1 \bmod p$

D. Point multiplication

Point multiplication of an integer n and a point p is defined as $np=p+p+\ldots+p$ (n times) while there exist fast algorithms to compute point multiplication based on point doublings.

LITERATURE REVIEW

For the security of fingerprint image information, various techniques have been developed in this emerging research area recently.

According to review article of A. K. Jain, K. Nandakumar, A. Nagar [3] template protection approaches were classified into three main categories: feature transformation, biometric cryptosystem, and hybrid systems. G.Panchal and D. Samanth[4] proposed an encryption method by extracting statistical feature to generate a codeword. Then by using Reed-Solomon encoding they convert that codeword to the key for their encryption scheme which means the key is generated from the original fingerprint image. C. Moujahdi, G. Bebis, S. Ghouzali and M. Rizza [5] proposed an approach to protect fingerprint template. They exploit the information provided by the extracted minutiae to construct a new representation based on special spiral curves which are stored in the database system to be used for recognition. 2D chaotic sequences from multi-scroll chaotic attractors were used for encryption by F. Han, J. Hu, X. Yu, and Y. Wang [6]. Encryption technique using minutiae-based transformation was proposed by Haiyong Chen and Hailiang Chen [7]. In this algorithm, a circular region around each minutia is constructed and non-invertible transformation is applied to all minutiae regions while all transformations are stored in the database. S. Zhao, H. Li and X. Yan [8] proposed a scheme combining with shuttle operation and nonlinear dynamic chaos system. G. Mehta, M. K. Dutta, J. Karasek and P. S. Kim [9] proposed a method based on chaotic theory using Arnold and Henon maps for generating cipher image. H-I Hsiao and J. Lee [10] proposed to combine four chaotic systems for encryption including two 1-D and two 3-D chaotic systems.

PROBLEM STATEMENT

All these algorithms used large key sizes. One of the biggest advantages of using ECC for encryption is that ECC usually require much smaller key sizes to achieve an analogous security level compared with the above schemes and other existing techniques. On the other hand, we almost have an unlimited source of elliptic curves which can be used for ECC. Actually, ECC Brain Pool [11] and National Institute of Standards and Technology (NIST) [12] provide various recommended and secured elliptic curve parameters of different bit sizes for researchers. Fingerprint images we have used here are obtained from Biometric Ideal Test (BIT) [13].

Some of the above-mentioned methods use random key generation techniques where keys are usually generated from pixel values. The problem arising here is that random key generation cannot generate the same key in two or more sessions which means their methods are not capable to meet the requirements in many application situations.

ISSN 2349-0292
Impact Factor 3.802

Many standard cipher systems such as IDEA and RSA are not suitable for practical fingerprint encryption because of their relatively large key sizes and high computational complexity.

In this work, we propose a new method to overcome the above issues by developing an adapted version of ECC procedure which inherits the advantages of being fast and secure of the general ECC schemes. Moreover, to enhance the overall confusion effect during encryption, we propose to add a pre-processing technique before applying the main ECC encryption algorithm. In particular, we use Arnold Cat Map for initial permutation which shuffles pixels in the original fingerprint images before applying ECC and this enhances remarkably the overall performance of our algorithm. Furthermore, in this research we use big prime fields on which we can deal with very big numbers at one time. This also enables us to incorporate block cipher techniques to reduce the computation time for encryption and decryption and increase the flexibility of our scheme.

PROPOSED METHOD

Since fingerprint encryption is a special category in the image encryption field, we should concern about image encryption processes for this special type of images. Our algorithm can be stated in a few main steps: applying ACM; selecting prime fields and coefficients for elliptic curves; dividing the image into blocks; and the final overall encryption and decryption algorithms.

A. Arnold Cat Map (ACM)

ACM is a 2D linear permutation of pixel locations with a chaotic behavior. Discrete Cat Map is used to demonstrate behavior of Poincare Recurrence of an image. Based on the image size, after a certain number of iterations of ACM the original image will be restored. As in the example shown in Fig. 1, after applying ACM on a fingerprint image (60×80 pixels) 60 times, the image is restored. To get a good confusion and diffusion in encryption, we may choose to apply ACM for 40 iterations.

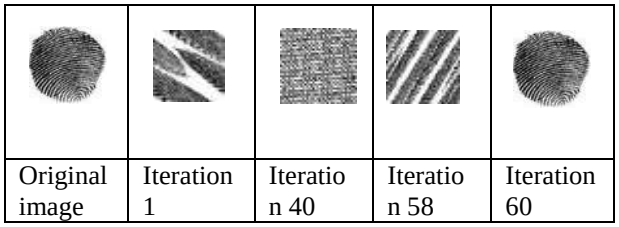


Fig. 1 A few iterations of ACM

B. Prime fields and curve coefficients

For 128 bit, 256 bit and 512 bit, prime fields of those bit sizes and other elliptic curve parameters are respectively chosen from some standard elliptic curves given by ECC Brain pool [11].

The domain parameters for a selected elliptic curve $y^2=\{x^3+ax+b\}\ mod\ p$ is (p,a,b,G,n) where p is the prime number for the underlying prime field of the elliptic curve, a and b are curve coefficients, G is called generator which is a point of the curve, n is the order of generator in the group of the elliptic curve.

C. Dividing blocks

The following table lists the block sizes we choose with respect to corresponding bit sizes. For each pixel, the pixel value is of 8 bit. We combine and convert pixel values in each block into one big integer, while it should be considered as an element of the prime field for the chosen elliptic curve of the corresponding bit size.

Table. 1. Block sizes

	Block size	# pixels
128bit	4×4	16
256bit	4×8	32
512bit	Used command Length[IntegerDigits[P512,256]]-1	63

ISSN 2349-0292
Impact Factor 3.802

D. Encryption and decryption

The overall encryption algorithm is summarized in the following (Algorithm 1). Our input includes the selected elliptic curve (Step B) and the fingerprint image for encryption. We first apply ACM (Step A) for initial permutations of the image pixels. Then we divide the image matrix into blocks and for each block a big integer is generated (Step C). Next, we want to apply ECC to each big integer. In particular, we combine Koblitz's Encoding Method [15] which is used to map each big integer to a point on the elliptic curve and a formal approach of ECC for general image encryption [16]. The output is the cipher data composed of a bunch of cipher points, one for each block. Moreover, for the purpose of illustration, we can generate the cipher image from the cipher data.

Algorithm 1: Fingerprint image encryption

Input : Elliptic curve parameters (p,a,b,G,n) and fingerprint images
Output : (X_{Mi},Y_{Mi}) where i= number of sub-matrixes (blocks)

1. Image → Pixel-value matrix;
2. Apply ACM;
3. Dividing into blocks (Table 1);
4. Pixel values in each block converted to a big integer;
5. Point 1 = Map the big integers to points on the elliptic curve using Koblitz's Encoding Method;
6. Select a random integer K from [$1,n-1$] and a public key P_b which is a randomly selected point on the curve;
7. Point 2 = Point multiplication of K and P_b;
8. Compute X_{Mi} as point multiplication of K and G;
9. Compute Y_{Mi} as point addition of Point 1 and Point 2;
10. Cipher points (X_{Mi},Y_{Mi}) for all i;
11. For illustration, a cipher image can be generated from cipher points block by block.

The decryption algorithm is summarized in the following (Algorithm 2). Note that ACM can also be run at the end of the algorithm.

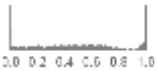
Algorithm 2: Fingerprint image decryption

Input : Elliptic curve parameter (p,a,b,G,n) and cipher data
Output : Original fingerprint

1. Divided to blocks according to the encryption block size;
2. For all blocks, run ACM of m-r iterations where m is the order of image and r is the number of iterations run in encryption;
3. Point 3 = Big integer from each cipher block;
4. Select client private key K_{pvt} from [$1,n-1$];
5. Point 4 = Point multiplication of $K \cdot K_{pvt}$ and G;
6. Compute point subtraction of Point 3 and Point 4
7. Fingerprint = Join all blocks in order and then convert to image

IMPLEMENTATION AND RESULTS

As a tool of implementation, we use Mathematica (version 11). As an example of the results, some fingerprint images, cipher images after encryption and their corresponding histograms are shown in the following figure. Meanwhile, we also apply the encryption to the benchmark Lena's image.

image	histograms	Cipher image	Cipher histogram
			

ISSN 2349-0292
Impact Factor 3.802

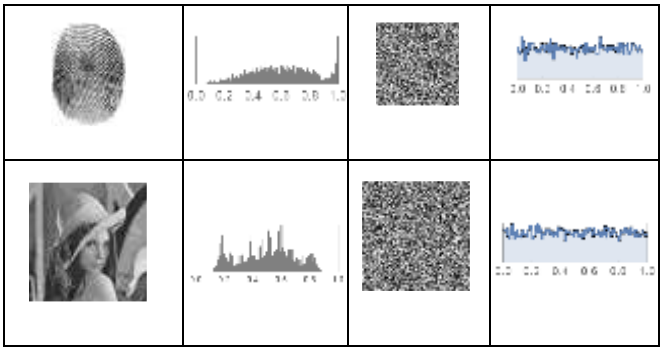


Fig. 2 Some encryption results

DISCUSSION AND SECURITY ANALYSIS

Security analysis of a cryptographic algorithm is crucial to ensure the strength of the used technique. To ensure the security of our fingerprint encryption method, several widely used factors are considered here, including NPCR (Number of Pixel Change Rate), UACI (Unified Average Charging Intensity), histogram analysis, speed analysis, keyspace analysis, performance under known plaintext and chosen plaintext attacks. In particular, we discuss the results from our full algorithm together with results from a partial algorithm where ACM is not performed.

NPCR and UACI test

An important requirement of the security of an encryption technique is that small changes of the plain image should result in a highly changed cipher image. For example, this requirement demonstrated by Y. Wu, J. P. Noonan and S. Agaian [17] were measured by using the standard tool, i.e., NPCR and UACI. We do such an analysis on our algorithm by averaging values over 53 randomly chosen fingerprint images with results being shown in Table 2.

Table.2. NPCR and UACI values tests on our scheme

Bit Size	**Block Size**	**ACM**	**NPCR (mean)(%)**	**UACI (mean)(%)**
128	19 pixels	No	99.65	33.60
		Yes	99.73	33.41
256	34 pixels	No	99.62	33.12
		Yes	99.71	33.64
512	63 pixels	No	99.66	33.07
		Yes	99.71	33.20

For all bit sizes, our algorithm consistently gives NPCR values of around 99.65% without ACM and values of more than 99.7% with ACM. This means incorporating ACM in encryption enhances the security performance of the algorithm.

Histogram Analysis

Good cipher images are generally required to have a close-to-uniform distribution of pixel values which is white-noise-like. As having been shown in Fig. 2, we can see that even though the original images have different types of image histograms, the cipher image histograms are always close to a uniform frequency distribution. No information is directly readable from the cipher images since they always appear as white noises.

Speed Analysis

The computational time depends on various factors such as the size of image, the operating systems, performance of the computer, programming languages, the algorithms themselves etc. We have implemented our algorithm in Mathematica version 11, execution time of encryption and decryption for fingerprint images is given by the following table whose values are taken from the average of the encryption /decryption of 53

fingerprints. Computational time of this proposed encryption and decryption algorithm is low with comparing with other methods [17].

Table. 5. Computational Time

Bit Sizes	Encryption Time (sec.)	Decryption Time (sec.)
128	0.5716	0.10937
256	0.6390	0.15625
512	0.6800	0.25

Finally we proposed encryption by simplified ACM with maximum number of pixel blocks as better scheme. Above Figures are explained it well. Proposed algorithm has very small time variation in particular class such as 0.0625, 0.03125, and 0.09375 for 128-bit, 256-bit, and 512-bit classes respectively. Therefore our algorithm is stable scheme.

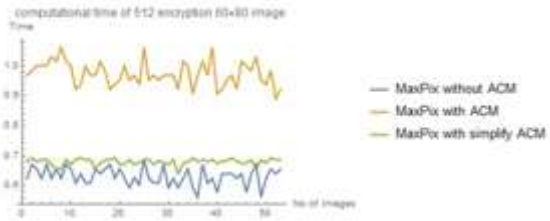


Fig.3 512bit encryption: Simplified ACM: 60×80 size images

Keyspace Analysis

To find the key used to encrypt image the fundamental way of cryptanalysis is brute-force attack. As stated in Algorithm 2, the private key use for decryption is chosen from [*1,n-1*] where n is the order of the generator *G* which is typically about the size of the underlying prime field. This means that for the used bit sizes of 128 bit, 256 bit and 512 bit, the keyspace is of 128 bit, 256 bit and 512 bit respectively while 128 bit keyspace is generally considered as secure with respect to brute-force attack.

Known plaintext and *chosen plaintext attack* have been used to crack some encryption algorithms. For example, some intruders have used all black and all white image for the searching pattern of the algorithm. In Fig.4, we show the cipher images of pure white and pure black plaintext images which are both white-noise-like with no informative patterns visible. Therefore we expect our algorithm to be highly resistant to these types of attacks.

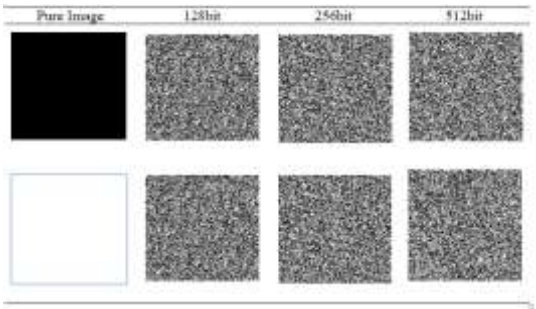


Fig.4 Pure dark image and pure white encryption

CONCLUSIONS

In this paper, a new method is proposed for any kind of biometric images and specially for fingerprint encryption. Our algorithm is performed by combining an ECC type of image encryption and ACM. We have also done several conventional tests of security analysis on the proposed encryption/decryption scheme. In particular, the ACM procedure provides a 2D shuffle of the image pixels with a chaotic behavior which enhances the confusion effect of encryption. The specially designed ECC procedure which incorporates block

cipher techniques in our algorithm utilizes the advantages of general ECC techniques, e.g., relatively smaller key sizes, high speed process and high security. In addition, our algorithm provides options in choosing key sizes and block sizes which enables a flexible balance of computation resources and meeting higher security requirements. We conclude that the proposed algorithm has a great performance in both efficiency and security which is highly practical for fingerprint data storage and transmission through unsecure networks.

REFERENCES

[1] N. Koblitz, "Elliptic Curve Cryptography" Mathematics of Computation, AMS, vol. 48, no. 177, pp. 203-208, 1987
[2] V. Miller, "Uses of Elliptic Curve in Cryptography", Advanced in Cryptology, Springer-Verlag vol. 85, pp. 417-426, 1986
[3] A. K. Jain, K. Nandakumar, A. Nagar, "Biometric template security", Advances in Signal Process, EURASIP journal, vol. 2008, pp. 1-17, 2008
[4] G. Panchal and D. Samanta, "A novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Application to storage security", Computer and Electrical Engineering 000, Elsevier, pp. 1-18, 2018
[5] C. Moujahdi, G. Bebis, S. Ghouzali and M. Rizza, "Fingerprint shell: Secure representation of fingerprint template", Pattern Recognition Letters 24, Elsevier, pp. 189-196, 2014.
[6] F. Han, J. Hu, X. Yu and Y. Wang, "Fingerprint image encryption via multi-scroll chaotic attractors", Applied Mathematics and Computation 185, Elsevier, pp. 931-939, 2007.
[7] Haiyong Chen and Hailiang Chen, "A novel algorithm of fingerprint encryption using minutiae-based transformation", Pattern Recognition Letters 32, Elsevier, pp. 305-309, 2011.
[8] S. Zhao, H. Li and X. Yan, "A secure and efficient fingerprint image encryption scheme", The 9th International Conference for Young Computer Scientists, IEEE Computer Society, P.R.C, pp. 2803-2808, 2008
[9] G.Mehta, M. K. Dutta, J. Karasek and P. S. Kim, "An efficient and lossless fingerprint encryption algorithm using Henon Map & Arnold Transformation", International Conference on Control Communication and Computing, IEEE, pp. 485-48, 2013.
[10] H-I Hsiao and J. Lee, "Fingerprint image cryptography based on multiple chaotic system", Signal Processing 131, Elsevier, pp. 169-181, 2015.
[11] ECC Brainpool Standard Curves and Curve Generation v.1.0, 19.10.2005
[12] www.csrc.nist.gov
[13] http://biometrics.idealtest.org
[14] Y.Wu, P.Noonan and S.Agaian, "UPCR and UACI randomness test for image encryption", Cyber Journal, pp. 31-38, 2011.
[15] O. Reyad and Z. Kotulski, Image encryption using Koblitz's encoding and new mapping method based on elliptic curve random number generator, Springer International Publishing, Switzerland, 2015, pp. 34-45.
[16] D. Hankerson, A. Menezes and S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2004.
[17] Y. Wu, G. Yang, H. Jin and J.P. Noonan, "Image encryption using the two dimensional logistic chaotic map", Journal of Electronic Imaging, vol. 21(1), 013014, March, 2012.
[18] S. Toughi, M. H. fathi and Y. A. Sekhavet,, "An image encryption scheme based on elliptic curve pseudo random and Advanced encryption system", Signal processing, vol. 141, Elsevier, pp. 217-227, 2017.
[19] X. Wang, X. Zhu and Y. Zhang, "An image encryption algorithm based on Josephus Traversing and mixed chaotic map", IEEE, 2018.