Signal Processing 141 (2017) 217–227

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

# An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System

Shahryar Toughi[a], Mohammad H. Fathi[a,*], Yoones A. Sekhavat[b]

[a] Faculty of Electrical and Computer Engineering, University of Tabriz, 29 Bahman Blvd., Tabriz, Iran
[b] Faculty of Multimedia, Tabriz Islamic Art University, Azadi Blvd, Hakim Nezami Square, East Azerbaijan, Tabriz, Iran

ARTICLE INFO

*Article history:*
Received 6 January 2017
Revised 3 April 2017
Accepted 9 June 2017
Available online 15 June 2017

*Keywords:*
Image encryption
ECC
AES
Random generator

ABSTRACT

Elliptic Curve Cryptography (ECC) has proven to be an effective cryptography. ECC has its own advantages such as efficient key size compared to other Public Key Infrastructures. This paper exploits the Elliptic curve random generator defined by National Institute of Standards and Technology (NIST) to generate a sequence of arbitrary numbers based on curves. The random generation phase is based on public shared key and a changing point G, which is a generator of a curve to obtain random sequences. Then, Advanced Encryption System is applied to these sequences acquiring arbitrary keys for encrypting image. Using AES alongside well distributed randoms provides a prominent encryption technique. Our experiments show that the proposed method fulfills the basics of cryptography including simpleness and correctness. Moreover, the results of the evaluation prove the effectiveness and security of the proposed method.

## 1. Introduction

Images are an inseparable part of our life. The joy of sharing these images has become so easy with the advent of Internet. On the other hand, the Internet is an open network which is not safe. Some images are confidential (e.g., militant and medical images) that must be kept out of reach from unauthorized users and adversaries. Therefore, there is a need for a secure image sharing method that guarantees safe image delivery. Cryptography plays a major role to achieve this goal. Various cryptography methods are proposed for image encryption using symmetric and asymmetric encryption methods [1], chaos system [1], DNA method [1], Arnold transformation [2], code computing [3], and hybrid methods of combining two or more of these methods.

In [4], an image encryption using hybrid AES (Advanced Encryption System) and ECC (Elliptic Curve Cryptography) is proposed, in which AES is employed for text encryption. In that paper, the focus is on the key sharing method, which was the encryption of AES key using ECC and the securing key using the digital signature of ECC. An improved version of this technique is proposed in [5], where an encryption method using hybrid AES-ECC is developed for wireless sensor networks. In this method, the generation of ECC key is followed by generating and encrypting an AES key using ECC. After transmitting this token to the other party, another pair of ECC key is generated (key #2) and encrypted using AES. Finally, this token is transmitted to the other party. The text is encrypted with ECC using key2 and *cipher*$_{ECC}$ is gained. Then, *cipher*$_{ECC}$ is encrypted using AES and the final ciphertext is obtained and transmitted through the network. The main drawback of this system is that the use of ECC for encrypting the whole plain text is time-consuming. Consequently, it is not efficient in terms of using energy, especially for weak sensors.

In [3], an image encryption method using code computing and ECC is proposed. In this technique, binary bits are mapped to Letters. Addition and subtraction operations are defined over letters, where an image is encrypted using letters, operations, and ECC. This method is vulnerable to the chosen plaintext attack, while the pattern is visible to the adversary. Moreover, full security analysis is not performed in [3].

In [6], a method for color image encryption is proposed that uses a combination of chaotic sine map, Chebyshev sine map, cat map, and logistic Chebyshev map in order to achieve good results for color image encryption. Chaotic sine map is used to obtain a substitution matrix. Using this matrix an S-box is generated which is applied to image encryption scheme. In the beginning, a cat map is applied to the plain image, and then substitution phase is performed using the generated S-boxes. The image is *Xored* with three random generated matrices which are obtained from the utilization of a logistic-Chebyshev map. Finally, a block permutation takes place using Chebyshev sine map to generate a block permutation random.

* Corresponding author.
*E-mail addresses:* mohammad.h.fathi@gmail.com (M.H. Fathi), sekhavat@tabriziau.ac.ir (Y.A. Sekhavat).

http://dx.doi.org/10.1016/j.sigpro.2017.06.010
0165-1684/© 2017 Elsevier B.V. All rights reserved.

In [7] Belazi et al. proposed a partial image encryption using chaos and linear fractional and lifting wavelet transform. First, an S-box is generated using Chebyshev map and addition, multiplication, division and subtraction in GF($2^8$) and generated pseudo random considered as an input for image encryption part. For ciphering plain image, LWT (Lifting Wavelet Transform) is applied to the image and then by using approximation coefficients, Tent map, logistic map and proposed S-box. Finally, inverse lifting wavelet decomposition is applied with details of coefficient vectors and approximation coefficients.

In [8], a method based on ECC is proposed, in which both parties compromise on ECC public parameters at the beginning. Then, this method adds a random decimal (1 or 2) to each pixel value. This continues with considering some pixel values together in order to find a big number and pairs them up (this is performed to improve the efficiency of the algorithm). These big numbers are the input of ECC algorithm. Then, a random number $K$ is multiplied to the public key of the receiver, and the result is added to pair numbers of the previous step. This converts the numbers into a range of 0 to 255 and sends them as an encrypted picture. In [9], a method based on ECC is proposed that employs the genetic algorithm to find the best optimum key. In this technique, the ECC is used to encrypt all pixels one by one. However, the use of ECC for each pixel and searching for an optimum key are expensive operations.

In [10], a hybrid encryption method using ECC and chaotic system is proposed. This technique employs cyclic elliptic curves with the help of an LFSR (Linear Feedback Shift Register) and chaotic system to generate keystream sequences. this technique encrypts a plain image that is converted to a 32-bit stream using the key streams. In [11], Liu and Liu proved that the method presented by El-Latif and Niu [10] is vulnerable to known plaintext and chosen plaintext attacks. To address this problem, they covered the errors by using Chirikov standard map [12] for the confusion/diffusion of the image. They also used a previous stream of cipher image in order to encrypt the next stream of the plain image. This method has some problems with the generated logistic map because there are correlations between $X_n$ values of the chaos system [13,14].

In this paper, we are motivated to propose a method which is safe while addressing the problems of previous works. In particular, we propose an image encryption scheme that takes the advantage of Elliptic Curve Cryptography (ECC) and Advanced Encryption System (AES) for image encryption. The proposed method uses ECC as a random generator, where a sequence of random numbers is generated based on ECC parameters. These randoms are used as inputs for AES key which generates key streams for image encryption. The procedure of random number generation is based on announced NIST (National Institute of Science and Technology) random number generation. Although NIST method is used widely, it has some drawbacks. The proposed random number generator in this paper addresses the drawbacks of this technique using a unique way of generating randoms by both Coordinates ($X$ and $Y$). To the best of our knowledge, no previous work has considered both $X$ and $Y$ coordinates for random number generation. However, we show using $Y$ coordinate improves entropy of generated random numbers. In the following, Section 2 presents a brief introduction to AES and ECC. Section 3 presents the details of the proposed method. Section 4 provides a complete analysis over the proposed method. Finally, Section 5 concludes the paper.

## 2. Mathematical preliminaries

A cryptosystem is based on mathematical rules. In addition, to use encryption algorithms, such systems must have an efficient key, which is large enough for key space. A good key generation requires a good mathematical foundation. In the following, techniques used for key generation in our technique are elaborated. Both of cryptography algorithms are secure enough nowadays. Elliptic curve cryptography is a PKI (Public Key Infrastructure) in which the key size is small enough to be used in every system. This feature allows the implementation of this algorithm on most devices. The second algorithm is AES, which is considered as a secure symmetric cryptography that is secure against known attacks. In this paper, by taking advantages of these two methods, a new cooperative framework is designed.

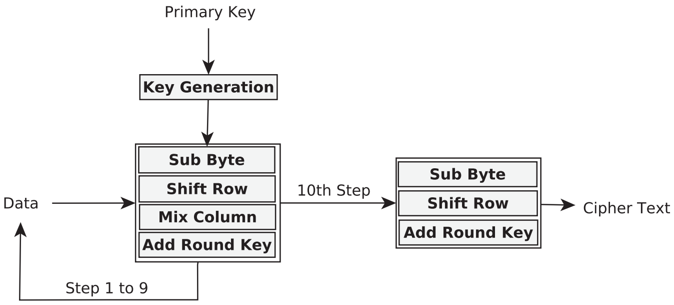

**Fig. 1.** Scheme for an 128-bit AES algorithm.

### 2.1. Advanced Encryption System (AES)

The AES cipher is also known as the block cipher Rijndael. No successful attack has been reported on AES. Some advantages of AES are easy to implement on 8-bit architecture processors and effective implementation on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). AES encryption is performed in multiple rounds. Each round has four main steps including sub-byte, shift row, mix column and add round key. Sub-byte is the substitution of bytes from a lookup table. Shift row is the shifting of rows per byte length. Mix column is multiplication over Galois field matrix. Finally, in the add round key step, the output matrix of mix column is XORed with the round key. The number of rounds used for encryption depends on the key size.

For a 128-bit key, these four steps are applied to 9 rounds, where the 10th round does not consider the mix column step. Since all steps are recursive, decryption is the reverse of encryption. Fig. 1 represents the AES algorithm including all steps.

### 2.2. Elliptic Curve Cryptography (ECC)

ECC is an asymmetric cryptography based on the public key. The security of this technique is promised by the discrete logarithm problem (DLP). ECC uses a smaller key size compared to RSA (Rivest Shamir Adleman). However, this small key size does not negatively affect the security of this technique. Because ECC uses a smaller key size, the calculations are performed faster (with considering low memory and computational power). The base formula for ECC is defined in Eq. (1) [15]:

$$y^2 = x^3 + ax + b \ (mod\ p) \tag{1}$$

Parameters $a$, $b$, and $p$ are publicly announced. For each $a$, $b$, and $p$ parameters, the modular space is changed based on $p$. Parameter $G$ is an initial point in Cartesian coordinate space on the curve, and it is also announced publicly in order to generate public keys. Two public and private keys are generated as follows. A random number is generated as a private key that is called $n_a$. The public key is obtained through multiplying $n_a$ and $G$. In an elliptic curve, multiplying is defined as a sequence of point additions. Some methods are presented to improve the multiplying