JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

A Novel Way for an Image Encrypt and Decrypt Using Parallel Computing

Dr. V J Chakravarthy[1] Dr.R.Vijayakumari[2]

[1]Principal, Arulmigu Kapaleeswarar Arts & Science College, Kolathur, Chennai - 99. chakkucksm1808@gmail.com

[2]Assistant Professor, Department of Computer Science , Krishna University, Machilipatnam vijayakumari28@gmail.com

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract

Since the advent of data communication over networks, it has become imperative to ensure security of information. Cryptography is a technique that is being employed. . In our previous paper[15] we made a concept on text oriented parallel signcryption (Cryptography). In this paper, it is shown how to adapt certain matrix transformation to create a novel asymmetric block encryption scheme. The proposed scheme is especially useful for encryption of large amounts of data, like digital images. First, a pair of keys is given by using matrix transformation; second, the image is encrypted using private key in its transformation domain; finally the receiver uses the public key to decrypt the encrypted messages. This scheme satisfies the characters of convenient realization, less computation complexity and good security. As a step towards the systematic application of public key cryptography, this article proposes an extension to the JCA framework to integrate threshold cryptography. Under this extension, various TC providers implementing different TC primitives can be plugged into a security application at run-time. This extension also makes it easy for an existing JCA-aware application to be migrated to use threshold cryptography. An example provider of threshold ECC is implemented under this framework extension. It is our belief that such an extension would help speed up the adoption of threshold cryptography.

Keywords: Security in Military and Air force, Threshold cryptography, Image Encryption Elliptic curve Threshold Cryptography, and Java cryptography architecture

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

1. Introduction

Nowadays, communication networks such as mobile networks and the Internet are well developed. However, they are public networks and are not suitable for the direct transmission of confidential messages. To make use of the communication networks already developed and to keep the secrecy simultaneously, cryptographic techniques need to be applied. Traditional symmetric ciphers such as Data Encryption Standard (DES) are designed with good confusion and diffusion properties [1]. These two properties can also be found in this paper which are usually erotic and are sensitive to system parameters and initial conditions. For image encryption,two-dimensional (2D) or higher-dimensional chaotic maps are naturally employed as the image can be considered as a 2D array of pixels [2-9]. In [2], Fridrich suggested that a chaos based image encryption scheme should compose of two processes: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with a 2D chaotic map while the latter alternates the value (gray-level) of each pixel in a sequential manner. By means of JCA we proposed the image into a 4 X 4 matrix transformations and then into grayscale image by meansof ECC-TC. Although measures such as pre-computation of permutation mode and sine tablewere suggested to reduce the computational complexity, the relatively slow diffusion process still limits the performance of this cryptosystem. To accelerate the encryption speed of Lian et al's cryptosystem and other ciphers based on the iterative confusion-diffusion processes, we propose to introduce certain diffusion effect in the confusion process so that this effect is not solely contributed by the slow diffusion process. Simulation results show that the number of overall rounds and hence the number of time-consuming diffusion processes is reduced without sacrificing the security level. The overall encryption time is shortened although the time required in the confusion stage is increased slightly.

Also, **IEJPC** focuses to achieve the lower bound in terms of time necessary to perform authenticated encryption, and decryption as well, or

time(ll_{rl} Enc & sgn) □ max {time(Enc),time(sgn)}

and

time(ll_{rl} Dec & ver) □ max {time(Dec),time(ver}

At best, the **IEJPC** would consume roughly the same time as the most time-consuming operation (either signing or encryption).

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

Furthermore, to meet the big gap between the state-of-the-art security research community and the state-of-the-art security practice. The paper proposes a 3-tier framework based on Java Cryptography Architecture (JCA) [10] for **IEJPC** services.

2. State of art research on AIEMT

Without loss of generality, we consider encrypting the grayscale image, named as IM×N (To RGB image, using its luminance space). The whole encryption process is described as follows:

Step 1: Creating the key pairs: private key for encryption, public key for decryption;

Step 2: Dividing original image into distinct P×P blocks and transforming them into DCT domain;

Step 3: Using the private key to encrypt the frontal
K × K coefficients of P×P every block;

Step 4: Making the inverse DCT transformation and uniting all P × P blocks;

Step 5: Deal with the transformed coefficients and keep them between 0 and 1.First, we create a set of orthonormal bases{ui, i = 1, 2, . . .K} of length P and an invertible matrix A of size P ×P by using the method of[11]. {ui} forms the column vector of U, defined as:

$$[A]=\begin{bmatrix} a11a12\ldots a1p \\ a21k22\ldots a2p \\ \vdots\ \vdots\ \vdots\ \ \vdots \\ ap1ap2\ldots app \end{bmatrix}$$

$$[U]=\{ui\ \}=\begin{bmatrix} u11a12\ldots a1k \\ u21k22\ldots a2k \\ \vdots\ \vdots\ \vdots\ \vdots \\ up1ap2\ldots apk \end{bmatrix} \qquad \textbf{(1)}$$

The private key and public key are AU and A^{-t} U, respectively, where A^{-t} denotes the inverse

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

transpose of A. The details of encryption and decryption are as following:

Encryption

Step 1: Dividing original image into distinct P × P blocks and transforming them into DCT domain, the corresponding DCT coefficients are named as $X_{M\times N}$.

$$\mathbf{X_{M\times N} = DCT\ (I, [P\ P])} \qquad \mathbf{(2)}$$

Step 2: Encrypting the frontal K×K coefficients of every P×P block, respectively. Let X1 denotes the matrix composed by the frontal K ×K coefficients of certain P ×P block X0, the corresponding encryption formula by using the private key AU can be described as:

$$\mathbf{X_2 = AUX1} \qquad \mathbf{(3)}$$

Step 3: Replacing the frontal P × K coefficients of X_0 with $X_2 \in R^{P\times K}$

If K is close to P, according to the characteristic of DCT coefficients, the rest (P − K) × (P −K) coefficients are all close to 0. So we can directly replace them and the decrypted image is almost not influenced.

$$\mathbf{X_0\ (i, j) = X2\ \{1\leq i \leq P,\ 1 \leq j \leq K\}} \qquad \mathbf{(4)}$$

Step 4: Making the inverse DCT transformation and uniting all P ×P blocks, the final result is defined as $X2_{M\times N}$.

$$\mathbf{X_{2M\times N} = IDCT\ (X_{M\times N})} \qquad \mathbf{(5)}$$

Step 5: Keeping all the transformed coefficients between 0 and 1.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

```
% Get the minimum of X2_{M×N},
  named as Min
Min = max((−1) × X2_{M×N})
% Ensure all the coefficien ts of X2_{M×N}
  more than 0
X2_{M×N} = X2_{M×N} + Min
% Get the maximum of updated X2_{M×N},
  named as Max
Min = max(X2_{M×N})
% Ensure all the coefficien ts of X2_{M×N}
  less than 1
X2_{M×N} = X2_{M×N} / Max
```

(6)

Step 6: Saving the encrypted image as bmp file.

Decryption

The decryption operation is a usual correlation process with five elements: (1) block length P;

(2) encryption matrix dimension K; (3) public key A^{-t} U; (4) the coefficient minimum Min; (5)the coefficient maximum Max. Suppose $X3_{M\times N}$ denotes the encrypted image, the details of decryption are following:

Step 1: Recovering all coefficients of $X3_{M\times N}$

$$\mathbf{X_{3\,M\times N} = X3_{M\times N} \times Max - Min} \qquad \mathbf{(7)}$$

Step 2: Applying DCT transformation to each distinct P × P block of $X3_{M\times N}$

$$\mathbf{X_{4\,M\times N} = DCT\,(X3_{M\times N},\,[P\ P])} \qquad \mathbf{(8)}$$

Step 3: Decrypting the frontal P ×K coefficients of every P × P block, respectively. Let D1 denotes the matrix composed by P ×K coefficients of certain P×P block D0, the corresponding decryption data D2 € $R^{K\times K}$ by using the public key A^{-t}U can be given as following:

$$\mathbf{=> D2 = (A^{-t}U)^t\ D1}$$

$$\mathbf{=> D2 = (U^tA^{-1})(AU)\ X0} \qquad \mathbf{(9)}$$

$$\mathbf{=> D2 = (U^tU)\ X0}$$

Because the column vector of U is a set of orthonormal bases, it is easily proved: U^tU = E. So,we can draw the conclusion:

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

$$\Rightarrow \mathbf{D_2 = X_0} \qquad \textbf{(10)}$$

Step 4: Replacing the frontal P × K coefficients of D_0 with D_2 and 0.

$$Do(i,j) = \begin{Bmatrix} D2\{1 \le t, j \le k\} \\ 0\{k \le i \le p, 1 \le j \le k\} \end{Bmatrix} \quad (11)$$

Step 5: Making the inverse DCT transformation and uniting all P ×P blocks, the final result is defined as $X5_{M\times N}$.

$$\mathbf{X5_{M\times N} = IDCT\ (X4_{M\times N})} \qquad \textbf{(12)}$$

Step 6: Saving the decrypted image as bmp file.

3. Proposed Optimal IEJPC

The proposed scheme with the assumption that a private key group set Us= {u_1, u2, u3 …un} exists with n signers, having equal authority to examine and sign, divides the whole message intot (1≤ t ≤ n) readable sub-message blocks. Each of these t participants needs only to examine and break the private key of their corresponding sub-message block. After receiving the block, the designated receiver first proceeds to recover the message by providing his own public key and verify it. The proposed scheme consists of the two phases as like the first scheme.

Encryption

There is a trusted SA responsible for selecting the following parameters and generating the users' private keys.

i. A finite field defined as F*p* elements, where *p* is a large prime number.

ii. A secure elliptic curve *E*(*Fp*) over *Fp*,

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

iii. a generator point $G \in E(Fp)$ whose order is a large prime number, q within $\sqrt{\ }$

iv. a one-way hash function h whose output is an integer

v. a secret polynomial:

$f(x)= e_{t-2} x^{t-2}+ e_{t-1} x^{t-1}+..+ e_0+ e_1 x \bmod q$

where $e_i \in [1, q-1]$ and i=0,1,…t-1;

$p \in 1 \in 2 \quad p$;

vi. the group private key $f(0)=e_0$ and group public key $Y_s=f(0)G$ of the signer group;

vii. the private keys $f(x_i)$ and the public keys $Y_i=f(x_i)G$ of all signers u_i (i=1,2…,n) in the signer group, where x_i is the public identification code of the signer u_i. when i ≠ j, $x_i \neq x_j$ the private key X_r and the public key $Y_r= X_r G$ of the specified receiver u_r.

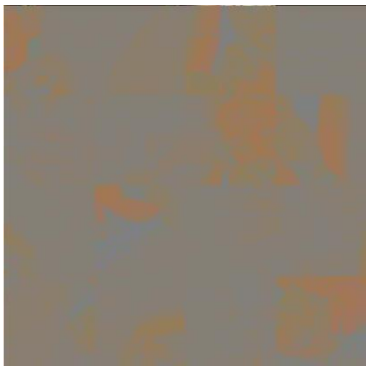
The parameters p, E, q, G, h, Ys, y_i and Y_r are then declared publicly. By means of the secret polynomial function we get the normal image as follows

Original Image

Public Key Image

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

Private Key Image [Encrypted]



Decryption

After receiving the group-private key block (r, s, r1, r2… rt), the receiver U_v performs the following procedure to recover the message blocks $\{m_1,m_2,\ldots m_t\}$, as follows.

Step-1: Compute the common session key Z shared with U_s, using the received (r, s), the public key Y_s of the signer group Us, and the private key x_v, as follows.

$Z= sY_v+(r.X_v)$ $Y_s =(x_z,y_z)$ (13)

Step-2: Recover the message blocks according to the following equation.

i. Compute

$$ut_{i1} = r_i.h(i \| x_z)^{-1} \bmod p$$

$$ut_{i2} = (y_z - s_i) \bmod q \qquad (14)$$

ii. Compute inverse transform

$k_{i2}= ut_{i2} \oplus \wp(ut_1)$ and

$k_{i1}= ut_{i1} \oplus \partial(ik_2)$ (15)

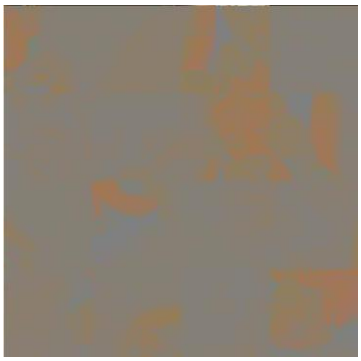
iii. Knowing two points $(1,ik_1)$ and $(2,ik_2)$, use the Lagrange interpolation and find the polynomial $\widetilde{F}(x) = a_0 + a_1 x \bmod p$

iv. Extract m_i from a_0 as follows $a_0=(m_i \| l_i)$

By means of the breaking code of private key sent by the user and the public key known by thet users the image can be recovered as follows

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

Decrypted Private Key Image



Decrypted Public Key Image

Original Image

4. JAC framework extension for IEJPC

JCA [10] and the Common Data Security Architecture (CDSA) are two cryptographicframeworks [12] for conventional public key cryptography. Neither of them supports group-

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

oriented cryptography. Recently JCA has been extended to support RSA based group-oriented cryptography [13]. The present work extends the JCA architecture to integrate the ECC based threshold cryptography, one of the most important types of group-base public key cryptography. The UML class diagram of TC based ECC framework extension is depicted in fig 1. Under this extension, various TC providers can be plugged into a security application at runtime. The extension also makes it easy for those JCA-based applications to easily be migrated to use threshold cryptography to enhance system security. It is our belief that this integration would speed up the adoption of threshold cryptography.

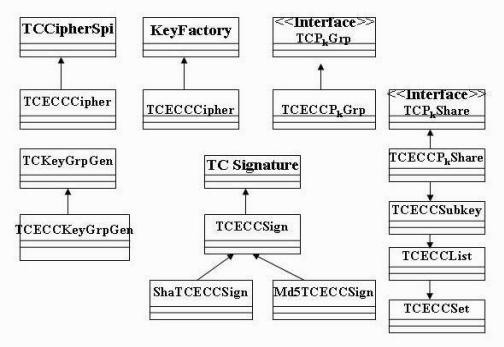


Figure 1: UML class diagram of ECC-TC framework

To test the above framework extension, we have implemented an example provider based on the threshold ECC algorithm [14], which can be used for threshold signcryption. The example provider has the following concrete classes:

- TCECCCipher inherits the TCCipherSpi and implements the threshold ECC algorithm. It is used in the threshold decryption and in the threshold co-signing as well.
- TCECCSgnextends the TCSgnSpiand provides the threshold signature service.
- TCECCGrpGen is defined to extend the TCKeyGrpGenSpi and used to generate key shares
- TCECCPvtKeyGroup extends the TCPvtKeyGroup and houses a collection of TCECCPvtKeyShr
- TCECCKeyFactoryextends the KeyFactorySpiclass

5. Conclusion

In large computer complexes, information security becomes a very pertinent issue. Furthermore in

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

applying layers of security, it is also crucial to conserve network resources such as processor time and memory. In our previous paper[15] we made research on text oriented parallel signcryption (Cryptography). This paper has attempted to propose the same parallel scheme in terms for image threshold encryption which would be superior to well-studied sequential scheme in terms of their efficiency, since they allow parallel encryption as well as parallel decryption. Besides, an attempt is made to improve the efficiency of the proposed scheme by dividing the message into several sub-blocks. The paper has endeavored to integrate the features of ECC and TC to provide the best of both worlds in information security. To bridge gap between the state- of-the-art security research community and the state-of-the-art security practice, a layered framework is proposed for IEJPC extending the functionalities of JCA. In future, we would evaluate the performance of the new scheme for various attacks in comparison to the well-known the existing schemes.

Reference:

[1] Schneier B. Cryptography: Theory and Practice. Boca Raton: CRC Press;

[2] Fridrich J. Symmetric Ciphers Based on Two-dimensional Chaotic Maps. Int. J.Bifurcat Chaos 1998;8(6):1259-84.

[3] Belkhouche F, Qidwai U, Gokcen I, Joachim D. Binary image transformation using two- dimensional chaotic maps. In: Proc ICPR 2004, Aug 2004, p.823-6.

[4] Guan ZH, Huang FJ, Guan WJ. Chaos-based image encryption algorithm, Phys Lett A 2005;346:153-7.

[5] Lian SG, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals 2005;26(1):117-29.

[6] Feng Y, Li LJ, Huang F. A symmetric image encryption approach based on line maps. In: Proc ISSCAA 2006, Jan 2006, p. 1362-67.

[7] Chen G, Mao YB, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 2004;12:749-761.

[8] Mao YB, Chen G, Lian SG, A novel fast image encryption scheme based on the 3D chaotic baker map. Int. J. Bifurcat Chaos 2004;14(10):3613-24.

[9] Lian SG, Sun J, Wang Z. Security analysis of a chaos-based image encryption algorithm, Physica A 2005;351:645-61.

[10] Sun Microsystem, "Java cryptography architecture API specification & reference", http://java.sun.com/j2se/sdk/1.3/docs/guide/security/CryptoSpec.html, 1999.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 5427-5438
https://publishoa.com
ISSN: 1309-3452

[11] T. Chuang and J. Lin,"A new multiresolution approach to still image encryption," Pattern Recognition Image Anal., Vol. 9, No. 3, pp. 431-436,1999.

[12] Y. M. Tseng and J. K. Jan, "An Efficient Authenticated Encryption Scheme with Message Linkages and Low Communication Costs", Journal of Information Science and Engineering,", 41-46, 2002.

[13] The Open Group, "Common security:CDSA and CSSM, version 2", http://www.opengroup.org/ publications/catalog/c914.htm.

[14] Y. Huang, D. Rine, and X. Wang, "A JCA-based implementation framework for threshold cryptography", Computer Security Applications Conference, IEEE Proc., 85-91, 2001.

[15] T.Karthick, R.S.Varalakshmi, V.Thavavel, V.Subburaj, "A Java framework for Optimal ECC-based Threshold Signcryption**"** Advanced Computing and Communication Technology for High