International Journal of Information Technology and Knowledge Management
July-December 2009, Volume 2, No. 2, pp. 245-248

EFFICIENT IMAGE ENCRYPTION USING MRF AND ECC

Kamlesh Gupta* **& Sanjay Silakari****

In this era, network security has become an issue of importance, on which lot of research is going on. We have proposed a two level image encryption method using elliptic curve cryptography (ECC) which has been made more efficient by Markov random field (MRF). In this method a texture image generated using seed by MRF. This seed is use as secrete key that generated by elliptic curve method. XOR method are used to concealed original image with texture image, the mixed image pixel is encrypted using ECC for transmission. The resulting system gives comparatively small block size, high speed and high security.

Keywords: Elliptic Curve Cryptography (ECC), Markov Random Field, (MRF), Gibbs Random Filed (GRF).

1. Introduction

In this world of multimedia, most of the devices are connected to the internet. In the development of 3G devices, all element of multimedia (text image audio and video) are used. To use this information, a channel of high bandwidth and more secured system is required.

Over last three decades, the traditional cryptosystem like DES, DLP, AES, DSA and RSA etc. are used for privacy and security. But these conventional methods are not able to support the new generation of digital communication and information access devices, these devices required a crypto-security technology.

A method called Elliptic Curve Cryptography is becoming the choice for mobile communication. Elliptic curve cipher use very small key size and computationally is very efficient. N. Koblitz and Miller, independently proposed the elliptic curve cryptosystem. A crypto-algorithm utilizes a discrete logarithm problem (DLP) over the point on an elliptic curve. ECC should be used to provide both digital signature and an encryption scheme.

Table 1
Comparison of the Equivalent Security Level for Some Commonly used Cryptographic Key Sizes

Time to break in MIPS years	*RSA/DSA Key Size*	*ECC Key Size*	*RSA/ECC Key Size Ratio*
10^4	512	106	5:1
10^9	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{79}	21000	600	35:1

Today, RSA is the powerhouse crypto-security of choice for E-commerce transaction. The RSA is too slow compared to ECC because ECC required smaller key size. The IT connectivity provides will be able to utilize fewer crypto-server securities for providing secure network connections. Table 1 compare the security level for some commonly considered crypto-graphics Key size.

2. Work Already Done in This Field

To achieve higher security of digital image RSA scheme with MRF and ECC Proposed for image encryption [Chaur -Chin Chen, 2004]. This paper proposed first encrypt original image with XOR concealed image that generate with MRF using seed and generate secret image using Elliptic curve Cryptography (ECC). XORing message again encrypted by RSA scheme.

In [Kefa Rabah, 2006] Elliptic curve cryptography scheme was Proposed and which is based on binary finite GF [2^m]. This work describe the basic design principal of ECC protocol like EC, Diffie-Hellman, EC Elgamal and ECDSA protocol. Unreliable network re-authentication protocol was proposed in [Sureswarn Ramadass *et.al.*, 2007], which is based on hybrid key using communication sequential process (CSP) and achieves high level of security via the use of public key cryptography scheme. The analysis of public key cryptography for wireless sensor networks security was proposed in [F. Amin *et.al.*, 2008], this work study he behavior of WSN nodes that perform public key cryptographic operation this evaluate time and power consumption of public key cryptography algorithm for signature and key management. This work presents the way in which hierarchy for the access to information in a user group on a communication channel in a layered structured was proposed in [Nicolae Constantinescu *et.al.*, 2007]. This work proposed authentication rank with identities based on Elliptic curve, it will be created the manner in which the two will authentify their self, by using secret information

* RJIT, BSF Academy, Tekanpur, Gwalior, M.P, India
E-mail: kamlesh_rjitbsf@yahoo.co.in

** UIT, RGPV Bhopal, MP, India. *E-mail: ssilakari@yahoo.co.in*

and arbitrary string which can be the names of two. On these strings and other data that will be added and competing for the final definition of the key.

The value encryption algorithm (VEA) was proposed in [Luminita Scripcariu *et.al.*, 2005]. The VEA could be applied using polynomial inversable function defined on GF(2^m). The statistical property of the encrypted image are compared to those of the originals. Correlation low, more secure for transmission, less processing time and less storage memory used in encryption. An image encryption for secure internet Multimedia application was proposed in [Philip P. *et.al.*, 2000]. This paper present a joint image compression and encryption scheme for internet multimedia application. The encrypted image is compared to those of the originals. More secure for internet multimedia transmission, less processing time and less storage memory used in encryption. A modified Ising model for generation binary image was proposed in [R.C. Dubes *et.al.*, 1989]. This paper uses the texture model of markov random field (MRF) in binary image generation using a seed. This seed use as a secret key in elliptic curve cryptography. This work was proposed modified Ising model by considering its parameter as a vector that depends on the neighborhoods of the image. The discrete algorithm problem is useful number theoretic problem in cryptography.

The co-diffie-hellman problem [Taiichi Saito *et.al.*, 2004] presents efficiently computable algorithms that generate the co-diffie-hellman problem over elliptic curves and proposed a special class of the co-diffie-helman. The mixed image element encryption using elliptic curve cryptography has been proposed in [Guiliang Zhu *et.al.*, 2008]. This work mixed two image elements using union operation and then applies elliptic curve cryptography for each mixed image element. This work proposed highly secured image element because it gives two-level encryption. The proposed work give mathematical model and structure model of mixed image element (MIE) encryption system that analyzes the efficiency and system security. ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange was proposed in [Levent Ertaul *et.al.*, 2005]. This work proposes a new approach to provide reliable data transmission with strong adversaries. We combine Elliptic Curve Cryptography and Threshold Cryptosystem to securely deliver messages in n shares. As long as the destination receives at least *k* shares, it can recover the original message. We explore seven ECC mechanisms, El-Gamal, Massey-Omura, Diffie-Hellman, Menezes-Vanstone, Koyama-Maurer-Okamoto-Vanstone, Ertaul, and Demytko. For secure data forwarding, we consider both splitting plaintext before encryption, and splitting cipher text after encryption. Also this work suggests exchanging keys between a pair of mobile nodes using Elliptic Curve Cryptography Diffie-Hellman. And compare the performance of ECC and RSA public key encryption. The ECC cryptosystem is more efficient and secured and reduce the computational time and power compare than RSA.

The traditional public key cryptosystems were based on multiplicative group or multiplicative group field. These methods were further modified to have elliptic curve over large finite field [Neal Koblitz *et.al.*, 1987]. The discrete logarithm problem on elliptic curve is likely to be harder than the classical discrete logarithm problem. This work is also discusses the primitive points on an elliptic curve modulo *p*, and give a theorem on smoothness of the order of the cyclic subgroup generated by a global point. This work defines the various texts imbedding method using elliptic curve cryptosystem.

3. MATHEMATICAL REVIEW

3.1 Markov Random Field (Mrf):

Let an $M \times N$ texture image, x be represented as a matrix whose elements take values from the set $A = \{0, 1, 2 \ldots. 255\}$. Let Ω be the set of all possible images and let $S = \{1, 2, \ldots MN\}$ be the sites of a matrix ordered by a raster scan. A Gibbs random filed (Grf) is a joint probability mass function defined on Ω such that

$$P(x) = e^{-U/x} / Z \qquad (1)$$

where $U(x)$ is called the energy function, and

$Z = \sum y \in \Omega e^{-U(y)}$ is called the partition function. A Markov random field is a *Grf* whose probability mass function satisfies the following conditions:

(a) **Positivity:** $P(x) > 0$, for all $x \in \Omega$

(b) **Markov Property**: For all $t \in S$
$P(X_t \mid \{X_r\}, r = t) = P(X_t \mid \{X_r\}, \mathrm{r} \in R_t)$
where R_t is the ordered set of neighbors of site t.

(c) **Homogeneity**: $P(X_t/R_t)$ does not depend on the site t. Figure 1 defines the relative sites and orders of the neighbors of a site t. A *Grf* and an *Mrf* are equivalent with respect to a specified neighborhood system [8]. A *Grf* is completely characterized by its energy function $U(x)$. In this paper, we adopt the generalized Ising model whose energy function is defined as

$$U(x) = \sum_{t=1}^{MN} F(x_t) + \sum_{t=1}^{MN} \sum_{\gamma=1}^{c} \left[H(x_t, x_t + r) + H(x_t, x_t - r) \right]$$

where $H(a, b) = H(b, a)$ and c depends on the size of the neighborhood. For example, $c = 4$ in the 2nd order neighborhood system [8]. In this paper, we use $F(x_t) \equiv 0$ and define

$$H(x_t, x_t + r) = \theta_r I(x_t, x_t + r) \qquad (3)$$

where

$$I(a,b) = \begin{cases} -1 & if\ a = b \\ 1 & if\ a \neq b \end{cases}\text{’}$$

Dubes and Jain [8] listed a good algorithm for sampling a *Grf* or an *Mrf* with known parameters.

t:–3	t:–2	t:+4
t:–1	t	t:+1
t:–4	t:+2	t:+3

Figure a

2	1	2
1	t	1
2	1	2

Figure b

Figure 1: The Relative Sites and Orders of Neighbors of Site *t*

3.2 Elliptic Curve Cryptography

We consider an elliptic curve over a finite field associated with a prime number $p > 3$ whose equation can be written as [12]

$$y^2 = x^3 + ax + b \tag{4}$$

where a, b are two integers which satisfy $4a^3 + 27b^2 \neq 0$ ($mod\ p$). Then the elliptic group, $Ep(a, b)$, is the set of pairs (x, y), where $0 \leq x, y < p$, satisfying the equation (5) with the point at infinity denoted as O. The binary operation * defined on the group $Ep(a, b)$ is calculated as follows.

Let $A = (x_1, y_1)$ and $B = (x_2, y_2)$ be in $E_p(a, b)$, then $A * B = (x_3, y_3)$ is defined as

$$x_3 \equiv \lambda^2 - x_1 - x_2 (mod\ p)$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 (mod\ p) \tag{5}$$

where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ \ A \neq B \\ \dfrac{3x_1^2 - a}{2y_1} & if\ \ A = B \end{cases}$$

An example of $E_{31}(1, 5)$ is given in Table

Table 2
Point on the Elliptic Curve $E_{31}(1, 5)$

(0, 6)	(6,14)	(12, 3)	(15, 4)	(21,7)
(0,25)	(6,17)	(12,28)	(15,27)	(21,24)
(1,10)	(7,13)	(13,13)	(16,5)	(25,0)
(1,21)	(7,18)	(13,18)	(16,26)	
(3, 2)	(11,13)	(14, 2)	(19,30)	
(3,29)	(11,18)	(14,29)	(19, 1)	

4. THE ENCRYPTION ALGORITHM

1. First we are take $M \times N$ binary image as a input X.
2. We use generalized MRF model for generate texture image Y, this image is generate using seed [8].

   This seed derived from ECC method used as a private key.
3. Perform XOR bitwise operation between image X and Y generate image W, this is a first level encryption.
4. Each pixel value of image W, that is called message m, can be converted into the coordinate (X_m, Y_m) that are the point on elliptic curve.

   $X_m = m \times k + J$,   here $J = 0, 1, 2, 3$ ………..

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

   Where m is message K is the random positive integer. $(X_{m,} Y_m)$ is a square modulo P, where P is the prime no. and $P \geq K \times m$.
5. Encryption/decryption system require a point on G and an elliptic group $E_p(a, b)$. User A select a private key n_A and generate a public *key* n_A G. To encrypt and send message p_m to B, A choose a random positive integer k and produce the cipher text C_m consisting of the pair of points.

   $$C_m = \{kG, P_m + kP_B\}$$

   where P_B is the public key of user B.
6. Decrypt the cipher text using the method

   $\{Pm + kP_B - n_B(kG) = Pm + k(n_BG) - n_B(kG)\} = Pm$

Encryption Model

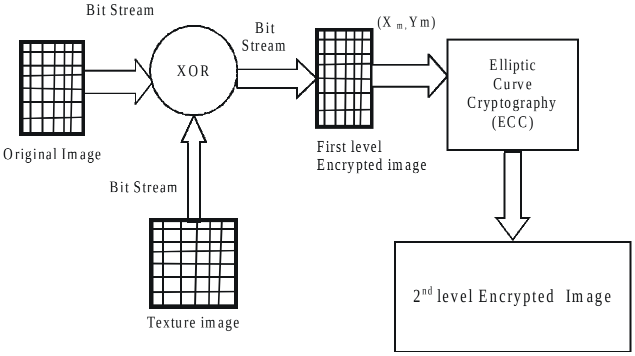
Bit Stream
Bit Stream
(X m, Y m)
XOR
Elliptic Curve Cryptography (ECC)
Original Image
First level Encrypted image
Bit Stream
Texture image
2nd level Encrypted Image

Figure 2 : Model of Two Level Image Encryption

5. EXPERIMENTS

For step (2), we synthesize a binary texture, **W**, from an Ising Markov random field with the authorized key Key = 121 which is derived from 2 × (12, 3) = 5 × (12, 28) = (1, 21) of an ECC,

$E_{31}(1, 5)$ with $G = (3, 2) \in E_{31}(1, 5)$ where $7 \times G = O\ (25, 0)$.

For step (3), the message shown in X is now hidden as $Y = X \oplus W$. For step (4), we transform the image Y pixel into (X_m, Y_m) coordinate that is the point of elliptic curve and then encrypted.

Shows the decrypted message by randomly guessing the Key = 123 instead of using the correct key = 121. Note that the original message will be completely recovered if the correct key is chosen.

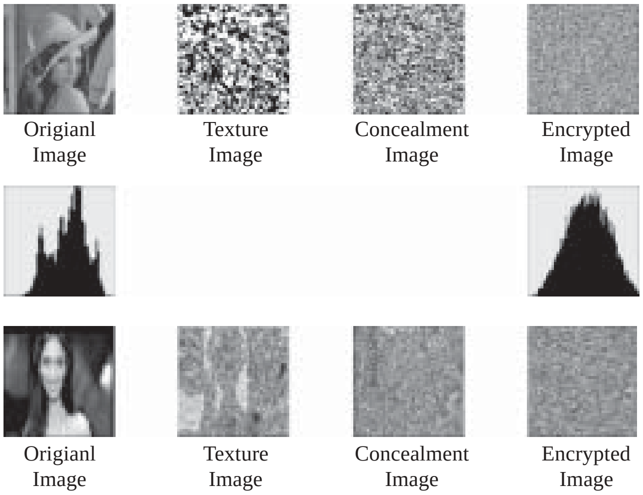

Figure 3: Two Level Image Encryption

6. Performance Evaluation

Apart from the image transmission consideration, some other issues on image encryption are also important. These include the running speed for real-time image encryption. The proposed image encryption is implemented using the compiler in Borland C^{++} development suite 5.0. Performance was measured on a 2.4 GHz Pentium IV with 256 MB of RAM running on Windows XP.

Table 3
Comparison of Different Image Encryption Time

Image Size (in pixels)	*No. of Colors*	*Encryption Time in Sec.*
256 × 256	16	0.05
256 × 256	256	0.09
256 × 256	16777216	0.12
512 × 512	16	0.25
512 × 512	256	0.32
512 × 512	16777216	0.45

5. Conclusions and Future Directions

This paper proposes a framework of using a cryptographic algorithm associated with an Ising *Mrf* texture model to cover a secret message to achieve information concealment before doing a conventional RSA data encryption. The issue is that the synthesized texture by an *Mrf* using the authorized key derived from elliptic curve cryptography is presumably difficult to be revealed. Furthermore, the *Mrf* parameters take floating point Numbers, which increases the complexity of intrusion. For the future work, some other texture models such as Gaussian *Mrf* models, fractal models, Gabor filters, and time series models may be used instead of Ising *Mrf* for information concealment under our proposed framework.

References

[1] Chaur-Chin Chen "RSA Scheme with MRF and ECC for Data Encryption". 0-7803-8603-5/04 IEEE, (2004).

[2] Kefa Rabah "Elliptic Curve Cryptography Over Binary Finite Field GF (2^m)". *Information Technology Journal* **5**(1) 204-229, ISSN 1812-5638, (2006).

[3] Sureswarn Ramadass, Rahmat Budiarto, and Ho Cheah Luan, "Unreliable Network Re-Authentication Protocol Based on Hybrid Key Using CSP Approach", *International Journal of Computer Science and Network Security,* (IJCNS)" **7**(11) (2007).

[4] F. Amin, A. H. Jahangir, and H. Rasifard, "Analysis of Public–Key Cryptography for Wireless Sensor Networks Security", *Journal of World Academy of Science,* Engineering and Technology, **31** (2008), ISSN 2070-3740.

[5] Nicolae Constantinescu, "Authentication Ranks with Identities based on Elliptic Curve", Annals of University of *Craiova Mathematics Computer Science Security,* **34**(1) (2007) 94-99, ISSN 1223-6934.

[6] Luminita Scripcariu and Mircea Daniel Frunza "A New Image Encryption Algorithm based on Inversable Functions Defined on Galois Fields", 243-246l, ISSN 0-7803-9029-6/05, *IEEE,* (2005).

[7] Philip P. Dang and Paul M. Chau, "Image Encryption for Secure Internet Multimedia Application", *IEEE Transaction* on Consumer Electronics, **46** (3) (2000) 395-403.

[8] R. C. Dubes and A. K. Jain, "Random Field Models in Image Analysis", *Journal of Applied Statistics,* **16** (1989) 131-164.

[9] Taiichi Saito and Shigenori Uchiyama, "The Co-Diffie-Hellman Problem over Elliptic Curves", Faculty of the Science and Engineering, Saga University, *Mathematics,* **33**(1) (2004) 1-8.

[10] Guiliang Zhu and Xiuaoqiang Zhang, "Mixed Image Element Encryption System", 9th IEEE International Conference for *Young Computer Scientists* ISSN 978-0-7695-3398, 1995-1600, (2008).

[11] Levent Ertaul and Weimin Lu, "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in *MANET* (I)", (2005) 102–113.

[12] Neal Koblitz, "Elliptic Curve Cryptosystem", Journal of Mathematics Computation, **48**(177) (1987) 203-209.