RSA Scheme With MRF And ECC For Data Encryption

Chaur-Chin Chen
Department of Computer Science
National Tsing Hua University
Hsinchu 300, Taiwan
Tel/Fax: +886 3 573 1078 / +886 3 572 3694
E-mail: cchen@cs.nthu.edu.tw

Abstract

The security of multimedia over network transmission has recently attracted a lot of researchers. This paper combines schemes of cryptography with steganography for hiding secret messages. Given secret messages, for example, an English sentence, our scheme first converts the messages to an $M \times N$ binary image which is then covered by a binary random texture synthesized from a 2D Ising Markov random field using the seed, a shared secret key, between the sender and the receiver, generated by the strategy of elliptic curve cryptography (ECC). The concealed messages are then encrypted based on the RSA scheme for transmission. An experiment shows that using an unauthorized key gets messages totally different from the original ones even the error key is very close to the authorized one.

Keywords: Elliptic curve cryptography, Markov random field, RSA

1 Introduction

In a digital multimedia era, the security of multimedia over network transmission and information concealment raises an increasing interest. The issues have been discussed in the E-commerce and Web-commerce society sporadically [11]. Recently, Petitcolas et al. [9] reported a survey of information hiding methods, Cox et al. [3] and Yu et al. [12] reviewed the watermarking techniques. As the technology moves, a hybrid scheme, based on combining the concept of *cryptography*, *steganography* and *watermarking* was investigated. Dittman, Wohlmacher, and Nahrstedt reported using cryptographic and watermarking algorithms [4]. Chen [1] adopted an Mrf texture image model [5] with RSA for hiding secret messages. This paper combines RSA, ECC [11], and Mrf to increase the difficulty of of attacks with the length reduction of cryptographic keys and a possible image texture cover.

Steganography [6] is a Greek ancient art of hiding information and is currently exploited to *either* put a digital image on the *secret messages* to hide the information or to insert *watermarks* [3, 12] into a digital image, audio, and video, to protect an intellectual property or to claim the copyright of ownership. The research of using steganography is to invent an intelligent use of camouflage such that no one except an authorized person can recover the secret messages.

Cryptography [8, 11], on the other hand, is concerned with strategies based on a *secret* key for hiding information. A well-known cryptographic system, RSA system [10], may encrypt a plaintext with a binary representation into a ciphertext with a public key (a, n), where $n = qr$ is a large number, $3 < a < m = (q-1)(r-1)$, and gcd(a, m)=1. Presumably, an RSA system realizes that only an authorized person knows how to factor n into the product of two primes, q and r, and so can he solve the private key b (that requires solving $ax \equiv 1 \ mod \ m$) to decrypt the ciphertext, The usage of RSA system is based on issuing a very large number $n = qr$ such that for intruders using trial and error approaches will never find the secret key b in their lifetime. On the other hand, the strategy of ECC [7] picks up the keys from the solutions of $y^2 = x^3 + ax + b$ over an integer finite field with a given prime number p under the condition $4a^3 + 27b^2 \ (mod \ p) \neq 0$. Given p, a, b, we can compute the set, $E_p(a,b) = \{(x,y)\}$, of the integer points on the curve. For examples, (3,2), (25,0), (12,28) are all in $E_{31}(1,5)$. If a user A picks up a *private key*, n_A (a positive integer), he can easily compute his public key, P_A in $E_p(a,b)$. Suppose that another user B wants to communi-

0-7803-8603-5/04/$20.00 ©2004 IEEE.

cate with A, he or she has to pick up a *private key*, n_B, computes and releases the public key, P_B. It can be shown that the same shared secret key between A and B can be done by evaluating $n_A \times P_B$ (or $n_B \times P_A$) under the operations defined on the integer points of $E_p(a, b)$.

This paper assumes that the secret messages are first converted and represented as a binary image. To hide the secrets by steganography, a synthesized texture, like a rain pattern, from a second order Ising Markov random field with parameters $(1, 1, -1, 1)$ [5] with the initial seed being an authorized key based on an ECC, $E_p(a, b)$ with known p, a, b, is generated to cover on the message by means of a simple image processing operation like "pixel exclusive-or" to encrypt and hide the secret message. Note that only the one who knows the exact authorized key can recover the information.

2 Mathematical Review

We briefly review the mathematical background of Markov random field texture models [5] and the elliptic curve cryptography [11] used in this paper.

2.1 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

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

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 $t \in S$, $P(x_t \mid \{x_r\},\ r \neq t) = P(x_t \mid \{x_r\},\ r \in R_t)$, 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 [5]. A Grf is completely characterized by its energy function $U(x)$. In this paper, we adopt the generalized Ising model whose energy funciton is defined as

$$U(x) = \sum_{t=1}^{MN} F(x_t) + \sum_{t=1}^{MN} \sum_{r=1}^{c} [H(x_t, x_{t:+r}) + H(x_t, x_{t:-r})] \tag{2}$$

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 [5]. In this paper, we use $F(x_t) \equiv 0$ and define

$$H(x_t, x_{t:+r}) = \theta_r I(x_t, x_{t:+r}) \tag{3}$$

where

$$I(a, b) = \begin{cases} -1 & if a = b, \\ \\ 1 & if a \neq b \end{cases} \tag{4}$$

Dubes and Jain [5] 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

(a)

2	1	2
1	t	1
2	1	2

(b)

Figure 1: The relative sites and orders of neighbors of site t.

2.2 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 [11]

$$y^2 = x^3 + ax + b \tag{5}$$

where a, b are two integers which satisfy $4a^3 + 27b^2 \neq 0\ (mod\ p)$.

Then the elliptic group, $E_p(a, b)$, 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 $\odot$ defined on the group $E_p(a, b)$ is calculated as follows.

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

$$\begin{aligned} x_3 &\equiv \lambda^2 - x_1 - x_2 \ (mod\ p) \\ y_3 &\equiv \lambda(x_1 - x_3) - y_1 \ (mod\ p) \end{aligned} \tag{6}$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & if\ A \neq B \\ \frac{3x_1^2 + a}{2y_1} & if\ A = B \end{cases} \tag{7}$$

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

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

Table 1: Points on the Elliptic Curve $E_{31}(1, 5)$.

3 The Algorithm

Suppose that a secret message to be hidden is converted and represented as an $M \times N$ binary image, X. We will implement the following steps.

(1) Issue an RSA public key (a,n), where n=qr, q and r are large prime numbers and let m=(q-1)(r-1). The conditions, gcd(a,m)=1 and ab≡1 mod m, must be satisfied [11].

(2) Use the generalized Ising Mrf model to generate a binary texture image W by the use of the authorized key Key obtained from an ECC as the initial seed for the Mrf synthesizer [1, 5].

(3) Cover the image X with W by Y=X⊕W, where each pixel of Y is obtained by $x \oplus w$, where $x \in X$ and $w \in W$ are the corresponding bit values.

(4) Get a word, y, an integer of k^2 bits long by rearranging a block of $k \times k$ pixels from the image, Y (the secret message covered by a binary texture).

(5) Encrypt each word obtained in (4) by the strategy of an RSA system to get the enciphered image Z.

(6) To decrypt and recover the message, an authorized person must know Key, the factors q and r of n, and the parameters of Mrf synthesizer which is extremely difficult although it is not unsolvable.

4 Experiments

To demonstrate how our algorithm works. Suppose that the message " *Vienna is a beautiful European city.*" is to be transmitted over the network. We first rearrange the message as shown in Table 2, then expands each character as a 8-bit string. So the message can be treated as a 6 × 48 binary image as shown in Figure 2(a).

For step (1), we select two prime numbers $q = 127$, $r = 193$; calculate $n = qr = 24511$, and $m = (q - 1)(r - 1) = 24192$. We further select $a = 1307$ which is relatively prime to m. Thus, $b = 10643$ is the unique solution of $ax \equiv 1\ mod\ m$.

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 $2 \times (12, 3) = 5 \times (12, 28) = (1, 21)$ 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⊕W which is shown in Figure 2(b).

For step (4), we first partition the image into 3×24=72 2×2 blocks, then pack each 2×2 block with bits y_0, y_1, y_2, and y_3 into a 16-bit integer by $y = 4096 * y_3 + 256 * y_2 + 16 * y_1 + y_0$.

For step (5), we encipher each y obtained in (4) as $z \equiv y^a\ mod\ n$ and then unpack the word z as four 8-bit integers to get the enciphered message Z as shown in Figure 2(c).

Figure 2(d) shows the decrypted message by randomly guessing the key $\widehat{Key} = 123$ instead of using the correct key $Key = 121$. Note that the original message will be completely recovered if the correct key is chosen.

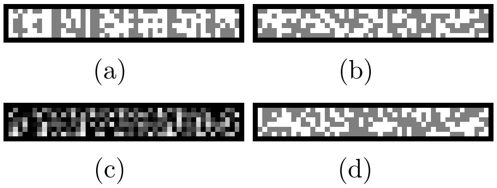
4.1 Discussion

It must be mentioned that the initial seed Key in step (2) of the generalized Ising Mrf plays a

V	i	e	n	n	a
	i	s		a	
b	e	a	u	t	i
f	u	l		E	u
r	o	p	e	a	n
	c	i	t	y	.

Table 2: A block representation for the messages.

very important role and can be changed any time due to the agreement of the persons who build the secret communication. As stated in step (2), we use ECC to compute the shared secret key based on the issued public keys and corresponding private keys from the persons who request the secret comunication. On the other hand, our experiment temporarily assumes that the public key (a, n) and the corresponding private key (b, n) are known to the persons who request a secret communication. The issue of key distribution can also be further overcome by the ECC or other strategies [11].


(a) (b)

(c) (d)

Figure 2: (a) Original, (b) Concealment, (c) Encipherment, (d) Decryption of an Intrusion

.

5 Conclusion

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 an 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 seriers models [5] may be used instead of Ising Mrf for information concealment under our proposed framework.

Acknowledgments: This work is supported by NSC Grant *92-2213-E-007-069*.

References

[1] Chen, C.C. (2001). Data Encryption Using Mrf with an RSA Key, *Lecture Notes in Computer Science*, LNCS-2195, 399-402.

[2] Chen, C.C. (2002). Watermarking experiments based on wavelet transforms, *The Proceedings of SPIE: Int'l Conference on Electronic Imaging and Multimedia Technology III*, Shainhai, China, Vol. 4925, 60-68.

[3] Cox, I.J., J. Kilian, T. Leighton, T. Shamoon (1997). Secure, spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, Vol. 6, 1673-1687.

[4] J. Dittman, P. Wohlmacher, and K. Nahrstedt (2001). Using cryptographic and watermarking algorithms, *IEEE Multimedia*, Vol. 2, 54-65.

[5] Dubes, R.C., A.K. Jain (1989). Random field models in image analysis, *Journal of Applied Statistics*, Vol. 16, 131-164.

[6] Johnson N.F., Jajodia, S. (1998). Exploring steganography: Seeing the unseen, *IEEE Computer Magazine*, Vol. 32, 26-34.

[7] Koblitz, N. (1987). Elliptic Curve Cryptosystems, *Mathematics of Computation*, Vol. 48, 203-209.

[8] Van Der Lubbe, J.C.A. (1999). Basic methods of cryptography, *Cambridge University Press.*

[9] Petitcolas, F.A.P., R.J. Anderson, and K.G. Kuhn (1999). Information hiding - A survey, *Proceedings of the IEEE*, Vol. 87, 1062-1078.

[10] Rivest, R., A. Shamir, L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems, *Communications of ACM*, Vol. 21, 120-126.

[11] Stallings W. (1999). Cryptography and Network Security: Principles and Practice, 2nd ed., *Prentice-Hall.*

[12] G.J. Yu, C.S. Lu, and H.Y.M. Liao (2002). A message-based cocktail watermarking system, *Pattern Recognition*, Vol. 36, 957-968.