DATA ENCRYPTION USING MRF WITH AN RSA KEY

Chaur-Chin Chen

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

Abstract

In a digital multimedia era, the security of multimedia over network transmission becomes a challenging issue. A strategy, combining cryptography with steganography, is investigated to overcome the problems in hand. This paper proposes hiding secret messages, represented as a binary image, by covering a binary random texture synthesized from a 2D Ising Markov random field with an authorized RSA key as the seed. Experiments show that an unauthorized key may never recover the message even it is close to the authorized one.

1 Introduction

The security of multimedia over network transmission and information concealment raises an increasing interest in a digital multimedia era. The issues are discussed in E-commerce and Web-commerce sporadically. Petitcolas et al. [5] reported a survey of information hiding methods. Cox et al. [1] and Wolfgang et al. [8] reviewed the watermarking techniques. As the technology moves, a new scheme, based on combining the concept of *cryptography* [4] and *steganography* [3] using a probabilistic texture image model, is investigated for hiding secret messages.

Steganography [3] 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 insert *watermarks* [1,6,9] into a digital image, audio, and/or video, to preserve an intellectual property or to claim the copyright. The research of using steganography is to invent an intelligent use of camouflage such that no one except the authorized person can read the secret message after *decryption*.

Cryptography [4], on the other hand, is concerned with strategies based on a *secret* key for enciphering or concealing data such as text, image, audio, and video data. A commonly

used cryptographic system, RSA system [7], based on Euler and Euclidean theorems from Number Theory, may encrypt a plaintext with a binary representation into a ciphertext with a public key (a, n), where $n = pq$ is a large number, $3 < a < m = (p-1)(q-1)$, 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, p and q, and so does 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 $n = pq$ such that for intruders using trial and error approaches can never find the secret key b in their lifetime.

This paper assumes that the secret message is represented as a binary image. To hide the secrets, a synthesized texture, like a rain pattern, from a second order Ising Markov random field with parameters $(1, 1, 1, -1)$ [2] with an authorized RSA key [4] as the seed covers on the message by means of a simple image processing operation like "pixel exclusive-or" to encrypt and hide the secret message. Only the one who knows the authorized key may recover the information.

2 The Algorithm

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

(1) Issue an RSA key (a,n), where n=pq, p and q are large prime numbers, m=(p-1)(q-1). gcd(a,m)=1 and ab≡1 mod m must be satisfied [4].

(2) Use an Ising Mrf model to generate a binary texture image W by the use of the authorized key b obtained in (1) as the initial seed for the Mrf synthesizer [2].

(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 pixels (bits).

(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 b, the factors p and q of n, and the parameters of Mrf synthesizer which is extremely difficult although not unsolvable.

3 Experiments

To demonstrate how our algorithm works. Suppose Figure 1(a) contains the original message which is a 64×64 0-1 binary image. We follows the algorithm.

For step (1), we select two prime numbers $p = 127$ and $q = 193$ such that $n = pq = 24511$ and $m = (p-1)(q-1) = 24192$. We further select $a = 2731$ which is relatively prime to m. Thus, $b = 18691$ is the unique solution of $ax \equiv 1 \ mod \ m$.

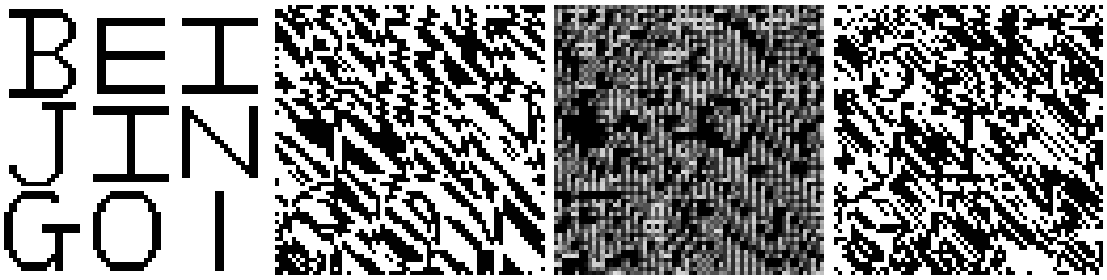
For step (2), we synthesize a binary texture, W, from an Ising Markov random field [2] with the authorized key $b = 18691$ as the initial seed.

For step (3), the message shown in X is now hidden as Y=X$\oplus$W as shown in Figure 1(b).

For step (4), we first partition the image into 32×32=1024 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 1(c).

Figure 1(d) shows the decrypted message by randomly guessing the key $\tilde{b} = 18693$ instead of using the correct key $b = 18691$. Note that the original message will be completely recovered if the correct key is chosen.



(a) (b) (c) (d)

Figure 1: (a) Original, (b) Concealment, (c) Encipherment, (d) Intrusion

.

4 Discussion and Conclusion

This paper proposes a framework of using a cryptographic algorithm associated with an Ising Mrf to cover a secret message to achieve information concealment. The issue is that the synthesized texture by an Mrf using the authorized key of an RSA system is presumably difficult to be revealed. Furthermore, the Mrf parameters are 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 [2] can also be used instead of Ising Mrf for information concealment under our proposed paradigm.

Other crytographic algorithms such as the one based on an elliptic curve [4] might also be considered.

References

[1] Cox, I.J., Kilian, J., Leighton, T., Shamoon, T.: Secure, spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, Vol. 6, No. 12, (1997) 1673-1687

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

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

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

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

[6] Pitas, I.: A method for watermark casting on digital images, *IEEE Trans. Image Processing*, Vol. 8, (1998) 775-780

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

[8] Wolfgang, R.B., Podilchuk, C.I., Delp, E.J.: *Proceedings of the IEEE*, Vol. 87, (1999) 1108-1126

[9] Website Digimarc, *http://www.digimarc.com*

[10] Website Stego, *http://www.stego.com*