ISSN 2250-3153

High Capacity Data Embedding Technique Using Improved BPCS Steganography

Ms. Pradnya R. Rudramath*, Prof. M. R. Madki**

*Electronics Dept., Walchand Institute of Technology Solapur, Maharashtra (INDIA)
Email: pradnyarudramath@gmail.com
**Electronics and Telecommunication Dept., Walchand Institute of Technology Solapur, Maharashtra (INDIA)
Email: mrmadki@yahoo.com

Abstract- The improved bit-plane complexity segmentation (BPCS) steganography carries on different processing's to different bit-planes, with setting high threshold value at the high bit-plane and low threshold value at the low. Steganography is an important issue in the filed of information safety. This paper concretely designs and carries out a steganography of the text secret information. RSA algorithm is used for encryption of the text secret information, so that others not privy to the decryption mechanism. The introduction of chaos theory conveniences to the test of steganography characteristics and enhance the safe of steganography. Not only provides good visual imperceptibility and data embedding capacity, this scheme also is capable of resisting the analysis of the whole histogram.

Index Terms- chaos; RSA; carrier image; text secret information; steganography; bit-plane blocks; threshold value

I. INTRODUCTION

IN recent years, information security issues have been paid more and more attention, and information hiding has become a hotspot in the research field of information security. Through embedding unnoticeable secrets into digital media signals such as images, audio and video, information hiding realizes the function of copyright protection and secret communication. Information hiding mainly consists of two main branches, which are digital watermark and steganography.

As an important branch of information hiding, steganography is mainly used in secret communication. It is an information security technology about secure transmission of secret information, which is using images, audio and other digital media as a cover [2], embedding the secret information to be sent into the carrier signal, transmitting as an unnoticeable way through public channels, especially the internet, aiming at sending out the information secretly and safely without causing suspicion of the behavior of hiding message.

The design of this paper is applied in secret information of text, and introduces chaos theory into steganography; it is easy to realize data encryption and simulation of binary data flow. RSA (Rivest, Shamir and Adleman) is an algorithm [7] for public-key cryptography. It is the first algorithm known to be suitable for signing as well as Encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

BPCS is the development of least significant bits (LSB) method, and it has better performance than the simple LSB method. The major idea is that multiple bit-planes of the cover images are divided into fixed-size blocks. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern; therefore, we can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. So this method has better visual imperceptibility.

Adopting an improvement type BPCS steganography with RSA and Chaos encryption, not only provides good visual imperceptibility and high data embedding capacity, this scheme also is capable of resisting the analysis of the whole complexity histogram.

II. RELATED WORK

In steganography, data is hidden inside a vessel or container that looks like it contains only something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files [10]. In recent years, several steganographic programs have been posted on Internet home pages. Most of them use image data for the container of the secret information. Some of them use the LSB of the image data to hide the data. Other programs embed the secret information in a specific band of the spatial frequency component of the carrier. Some other programs make use of the sampling error in image digitization. However, all those steganographic techniques are limited in terms of information hiding capacity. They can embed only 5-15 % of the vessel image at the best.

We have invented a new technique to hide text secret information in a color image. This is not based on a programming technique, but is based on the property of human vision system. Its information hiding capacity can be as large as 50% of the original image data. This could open new applications for steganography leading to a more secure Internet communication age. Besides, for the secret can be embedded in several bit-planes, compared with the LSB method it has greater data embedding capacity.

III. THE CONVERSION OF TEXT INFORMATION

The meaningful text messages need to be translated into encrypted binary data stream. The data stream is used for the embedding of carrier image, which makes preparations for the steganography. The conversion is shown as Fig. 1.

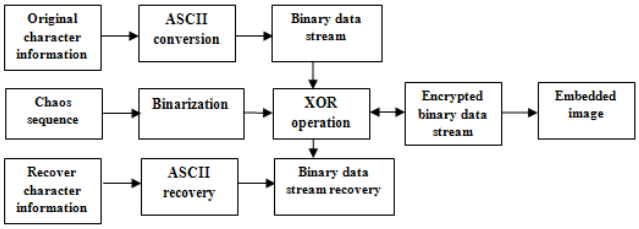


Figure 1: Conversion of text information

IV. RSA ALGORITHM

The RSA algorithm, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman, is currently one of the favorite public key encryption methods. RSA algorithm [7] is applied for the encryption of text information which is secure against a man-in-the-middle attack. It is very simply to multiply numbers together, especially with computers. But it can be very difficult to factor numbers. Steps involved in RSA algorithm:

A. Key generation:

1. Choose two distinct prime numbers p and q.
2. Compute $n = pq$.
3. Compute $\varphi(pq) = (p - 1)(q - 1)$. ($\varphi$ is Euler's totient function).
4. Choose an integer e such that $1 < e < \varphi(pq)$, and e and $\varphi(pq)$ share no divisors other than 1 (i.e., e and $\varphi(pq)$ are coprime).
   - e is released as the public key exponent.
5. Determine d (using modular arithmetic) which satisfies the congruence relation $de \equiv 1 \pmod{\varphi(pq)}$
   - d is kept as the private key exponent.

The **public key** consists of the modulus and the public (or encryption) exponent. The **private key** consists of the private (or decryption) exponent which must be kept secret.

B. Encryption:
$c = m^e \bmod n$
Where m is an integer $0<m<n$

C. Decryption:
$m = c^d \bmod n$

V. CHAOS THEORY

Chaos is a kind of behavior about nonlinear dynamics law control. This paper adopts Logistic mapping method to generate chaotic sequence:

$\alpha_{k+1}=\mu.a_k.\ (1-\alpha_k)$, k=0, 1, 2…..

The value traverses in the interval [0, 1], and μ is a control parameter or a bifurcation parameter. When 3.5699456….<μ<=4, the logistic map works in chaotic state. The data stream gene- rated is disordered, and it's similar to random noise.

The new binary sequence, which is the binarization of acquired chaotic sequence, has two main functions in this paper.

1. It is used to the encryption of text data information, steganography.
2. It is used to stimulate the binary data stream, which can facilitate the process of various experiments.

VI. IMPROVED BPCS STEGANOGRAPHY

A. BPCS steganography

The arithmetic of BPCS steganography is as follows:

1) The carrier image is divided into 8 different Bit-Planes. All the bit-planes are divided into small pieces of the same size, which is called bit-plane blocks, such as 8×8.

2) Calculate the complexity of every block. The complexity is defined as the amount of all the adjacent pixels that get different values (one pixel is 0, and the other is 1). The maximum possible value of the complexity is denoted as Cmax.

3) Setting the complexity threshold of the bit-plane block is αCmax, here α is a parameter. The bit-plane block whose complexity is larger than αCmax is used to embed secret information. The smaller the value of α, the more secret information can be embedded.

4) Secret information is formed into bit-plane blocks. The bit-plane block can replace the original one straightly if its complexity is greater than αCmax. Yet, it need to take conjugate processing with the checkerboard pattern block (as shown in Fig. 2) if the complexity is less than or equal to αCmax, than take the new block replace the original one.

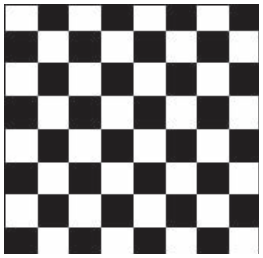


Figure 2: Checkerboard pattern block

5) Make a record of the blocks that have taken conjugate processing and this information also need to be embedded into the carrier. The embeddings of this extra information can not produce an effect on the embedded secrets, and it must be correctly picked up.

The process of secret information extraction is simple. Firstly, pick up all the pieces of the carrier data whose complexity is greater than αCmax, and then pick up the extra embedded information mentioned in step (5) to confirm the blocks that have taken conjugate processing. These blocks need take XOR operation with tessellated chock to get the recovery of secret.

B. Improved BPCS steganography

The original BPCS algorithm divides the carrier image into serious bit-planes, and there is high correlation between the bit-planes. The higher the bit-plane is, the stronger the correlation between the pixels of the bit-planes is [4]. So setting the same embedding strength for different bit-planes is sure to have an influence on the correlation between the bit-planes, leading to abnormalities of the complexity histogram, consequently, the security of steganography will be affect. Through detecting the complexity histogram, the analyst can analysis the existence of secret information, besides, he can estimate the embedding threshold value accurately [5]. In order to resist this statistical analysis method, this paper improves the BPCS algorithm.

The correlation of adjacent pixels is relatively strong when the bit-plane is high, and we can see the sketchy outline of the image. There is a certain degree of regularity among these pixels. Yet, the dates of the lower bit-planes are similar to random noise. Therefore, we shall make better use of HVS (human vision system) characteristic and consider the local characteristic of the image when embedding secret information, and treat different bit-planes with different way, with setting greater threshold for the higher bit-planes and smaller for the lower ones. Trough different bit-planes using different embedding strength, not only does this scheme resist statistical analysis, but also it can realize that embedding less secret information in higher bit-planes to have good visual imperceptibility and embedding more in lower bit-planes to have high data embedding capacity, solving the problem that keeps the balance on the contradiction between embedding capacity and visual imperceptibility.

Different bit-planes make different contributions to carrier image, this design sets greater threshold for the higher bit-planes and smaller for the lower ones.

VII. DESIGN AND IMPLEMENT

The technique of improved steganography text based on Chaos, RSA and BPCS designs as Figure 3.

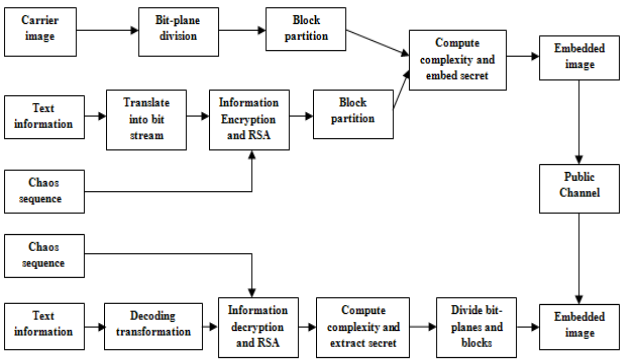


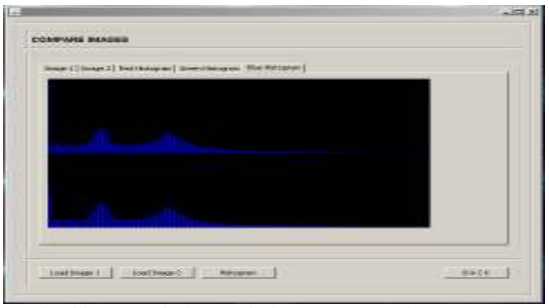
Figure 3: The technique of improved steganography text based on chaos, RSA and BPCS

VIII. ANALYSIS

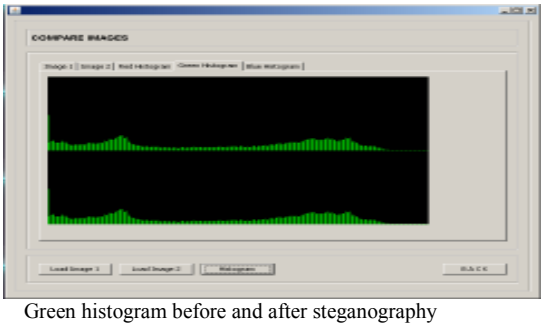
Select standard 24-bit "pepper" image

Figure 4: The image "pepper" before and after steganography

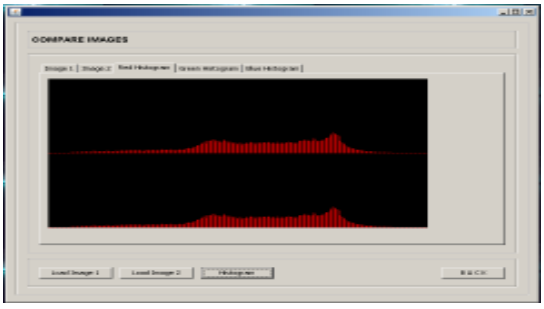
1) *Histogram measure:*



a) Blue histogram before and after steganography



b) Green histogram before and after steganography



c) Red histogram before and after steganography

Figure 5: Histogram measure before and after steganography

We can see that, there is no obvious difference in histograms before and after steganography. Then the design has high security.

IX. CONCLUSION

The main performances of steganography include visual imperceptibility and embedding capacity. The technique of improved steganography text based on chaos and BPCS apply to text secret information, the design has good visual imperceptibility and high data embedding capacity, and furthermore, it has a great advantage in resisting the analysis of the steganalysis. By introducing chaos theory and RSA algorithm, it is convenient to test the performance of steganography, and the design has higher security and reliability. Results show that the design of the paper has certain of theory value and application value.

REFERENCES

[1] Peipei Shi, Zhaohui Li, Tao Zhang, A Technique of improved steganography text based on chaos and BPCS, IEEE, (ICACC),2010,232-236.

[2] Wang S Z, Zhang X P, Zhang W M. Recent Advances in Image Based Steganalysis Research[J].Chinese Journal Of Computer, 2009, 32 (7): 1247-1263

[3] ZHANG H L, ZHANG X Y. A secure BPCS steganography against statistical analysis[C]. 8th International Conference on Signal Processing. 2006: 990-992.

[4] Wu J, Zhang R eta. Reliable Detection of BPCS Steganography [J]. Journal of Beijing University of Posts and Telecommunications, 2009, 32(4): 113-121

[5] ZHANG X P, WANG S Z. Statistical analysis against spatial BPCS steganography[J] . Journal of Computer- Aided Design &Computer Graphics, 2005,17(7):1625 – 1629

[6] Rivest, R.; A. Shamir; Adleman (1978). "A Method for Obtaining Digital Signature and Public-key Cryptosystems" (http://theory.lcs.mit.edu/~rivest/rsapaper.pdf). Communication of the ACM21:120-126.

[7] http://www.datahide.com/BPCSe/QtechHV-program-e.html

[8] Peipei Shi, Zhaohui Li, Tao Zhang, Statistical analysis against improved BPCS steganography, IEEE, (ICACC),2010,237-240.