논문 2009-46CI-1-10

스테가노그라피 기반에서 그레이코드를 사용한 비밀공유 기법

(Secret Sharing Scheme using Gray Code based on Steganography)

김 천 식*, 윤 은 준**, 홍 유 식***, 김 형 중****

(Cheonshik Kim, Eun-Jun Yoon, You-Sik Hong, and Hyoung Joong Kim)

요 약

인터넷 환경의 급속한 성장으로 인해 효율적인 디지털 콘텐츠 보급이 가능하게 되었다. 하지만 악의적인 공격자에 의한 저작권 침해 등으로 인해, 이미지 데이터 보호 및 비밀 통신 방법에 관한 요구사항 또한 높아지고 있다. Shamir와 Lin-Tsai는 각각 비밀 공유의 원리를 기반으로 간단한 비밀 이미지 암호화 알고리즘들을 제안하였다. 하지만, Shamir와 Lin-Tsai가 제안한 비밀 공유 기법들은 이미지의 화질을 저하시키는 심각한 문제가 있다. 이로 인해, 제3자가 쉽게 은닉된 정보를 알아챌 수 있다. 본 논문에서 이미지의 화질과 안전성을 향상시킬 수 있는 그레이 코드를 이용한 비밀 공유 기법을 제안한다. 제안한 기법은 Shamir와 Lin-Tsai의 기법들과 비교하여 공유 이미지의 화질이 우수할 뿐만 아니라 보다 강화된 보안성을 제공한다.

Abstract

Due to the rapid growth of the Internet, it is possible to distribute the digital content efficiently. However, the need for image data protection and secret communication technique is also on the rise because of an infringement of the copyright by malicious attackers. Shamir and Lin-Tsai proposed simple secret image encryption algorithms based on the principle of secret sharing, respectively. However, their secret sharing schemes have a serious problem which can be declined the image quality and it is possible for third party to know embed information. In this paper, we propose a new secret sharing scheme using gray code that can be increased the image quality and security. As a result of our experiment, the proposed scheme is not only shown of good image quality and but also provide enhanced security compare with Shamir and Lin-Tasi's schemes.

Keywords : Steganography, Secret sharing, Watermarking, LSB, BMP

I. Introduction

Steganography comes from the Greek words steganos, roughly translating to "covered writing"[1]. Steganographic techniques allow one party to communicate information to another without a third party even knowing that the communication is occurring. The ways to deliver these "secret messages" vary greatly. Therefore, steganography can be used to hide a message intended for later retrieval by a specific individual or group. In this case the aim is to prevent a message being detected by any other party. Steganographic techniques are often used by copyright holders who wish to combat theft. Images, video, and music can be encoded with information that can be used to identify the work as being the property of an individual or corporation. These encoding are often called watermarks.

*정회원, 안양대학교 교양학부
(Dept. of Liberal Arts, Anyang Univ.)
**정회원, 경북대학교 전자전기컴퓨터학부
(School of Electrical Engineering and Computer Science, Kyungpook National University)
***정회원, 상지대학교 컴퓨터공학과
(Dept. of Computer Science, Sangji Univ.)
****평생회원, 고려대학교 경영정보대학원
(Korea University)
접수일자: 2008년12월10일, 수정완료일: 2009년1월12일

Watermarked media can be distributed on the Internet while allowing copyright holders to be able to maintain their intellectual property. Commercially available watermarking technologies use robust techniques to encode information that are resistant to a variety of attacks on the message. Steganography and encryption are useful when you are used to ensure data confidentiality. However, the main shared feature between them is that both are used communicating for secret in public place. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret[2]. Recently, a lot of data hiding techniques have been developed by many researchers and improved it and also steganalysis has been advanced. Most steganalysis such as of Westfeld and Pfitzmann[3] was well known method to detect hidden message. It shows distortion from embedding hidden data.

Moreover, many people who were developing steganography tried not to detect a hidden message from cover images. However, new algorithm for detecting a hidden message is made by many researchers. Steganography is privately transferring method and very efficient method when communicating secret information of corporation, secret of military and secret of foreign policy. There is much method of sharing images proposed in many researchers.

Shamir[11] and Lin-Tsai[12] proposed simple secret image encryption algorithms based on the principle of secret sharing, respectively. However, their secret sharing schemes have a serious problem which can be declined the image quality and it is possible for third party to know embed information. In this paper, we propose a new secret sharing scheme using gray code that can be increased the image quality and security. As a result of our experiment, the proposed scheme is not only shown of good image quality and but also provide enhanced security compare with Shamir and Lin-Tsai's schemes.

Ⅱ. Related Works

These days, steganographic techniques are becoming strong in contrast to statistical attacks and undetectable by other varied attacks. For this reason, it was developed many steganography algorithms within a last decade. Among them, [4~7] are most favored. Nevertheless, many researchers have been interested in to crack steganographic schemes. Statistical attack was well known method to attack steganography because it is rather easy method. However, its solution is very simple, that is, it is possible to keeping the same or similar image histogram to the original image.

As proposed in [8], Chang and Hwang [9], Feng et al. [10], these image secret sharing schemes can produce both meaningful and meaningless stego-images based on the polynomial based (k,n) secret sharing scheme (Shamir, 1979)[11], depending on the application constraints and user's requirements. The so-called (k,n) secret sharing scheme, where $k \leq n$, the content of a secret message is divided into n shadows in the way that requires at least k shadows for the message reconstruction. Considering that the secret is an image, Shamir's polynomial-based secret sharing scheme performs well.

In [12], the prime number 251 was recommended in the calculation of (k-1)-degree polynomial to process the most range (0~250) in (0~255) for an 8-bit pixel. However, the gray scale value of secret pixel is constrained between 0 and 250. Although this results in the slight distortion of recovered image, we cannot actually get a lossless version of image secret sharing scheme. The problem is discussed and solved in Thien and Lin (2002)[8] using two pixels to represent (250~255). A proper choice should be Galois Field GF(28) instead of (mod 251) such that the calculation in (k-1)-degree polynomial can process the whole range (0~255) for an 8-bit pixel and no additional pixels are needed. The above three weaknesses show that Lin-Tsai scheme[12] is not an optimal solution for the qualities of the stego images

and secret image. In this paper, we proposed a new scheme that can overcome these weaknesses.

Ⅲ. Proposed Scheme

In this section, we describe our proposed embedding procedure and reconstruction procedure. The proposed scheme uses XOR(⊕) operation and gray code technique to enhanced the image security.

3.1 Gray code technique

Gray code is a form of binary that uses a different method of incrementing from one number to the next. With gray code, only one bit changes state from one position to another. This feature allows a system designer to perform some error checking (i.e. if more than one bit changes, the data must be incorrect). Table 1 below illustrates the difference between natural binary and gray code.

Gray codes are particularly useful in mechanical encoders since a slight change in position only affects one bit. Using a typical binary code, up to n bits could change, and slight misalignments between reading elements could cause wildly incorrect readings. An n-bit Gray code corresponds to a Hamiltonian cycle on an *n-dimensional* hypercube.

표 1. 그레이 코드
Table 1. Gray code.

Gray Code		Natural Binary	
0000	0	0000	0
0001	1	0001	1
0011	2	0010	2
0010	3	0011	3

3.2 Embedding procedure

Fig. 1 shows the proposed encoding algorithm that is used to embed a secret message into cover images. First, we choose cover images (CI_1, CI_2,$\cdots CI_n$) which are used to store secret message (*M*). Especially, *N* people have a different cover image for cryptography of secret distribution. The embed procedure is composed of six step for hiding secret messages (*M*)

```
Function Embedding (cover image (CI), messages (M))
  count =0
  SumCI(i, j) = CI1(i,j)⊕CI2(i,j)⊕,···⊕CIn(i,j)
  While (embed message, M)
  Begin
      If SumCI(i,j) ≠ M(index) then
      Begin
          CIcount(i,j) = NOT (CIcount(i,j))
                  count = count - 1
                  If count = 0 then count = 3;
      Else continue
      End
  End
  Count = 1
  [gray] = Bi2Gray([CIcount, CIcount+1, CIcount+2]);
  CIcount=gray[count]; // LSB substitution
  CIcount+1=gray[count+1]; // LSB substitution
  CIcount+2=gray[count+2]; // LSB substitution

  Number of N image created
  End
```

그림 1. 인코딩 절차
Fig. 1. Embedding procedure.

to number of *n* cover images (CI_1, CI_2,$\cdots CI_n$).

Step 1 : Select CI = {CI_1, CI_2,$\cdots CI_n$} and *M*.

Step 2 : Assign *count* to *n*, where *n* is number of CI.

Step 3 : Compute the following equation.

$$SumCI(i, j) = CI_1(i,j) \oplus CI_2(i,j) \oplus, \cdots \oplus CI_n(i,j)$$

Step 4 : Compare SumCI(i,j) with M(i,j). If two values are same, the message which we want to hide is stored to SumCI(i,j). Unless the two values are the same, compute the following equation and subtract *count* from one. If *count* value is *zero*, *count* variable should be initialized 0.

$$CI_{count}(i,j) = NOT\ (CI_{count}(i,j))$$

Step 5 : Transform LSB of pixel value in *CI* into gray code. *Bi2Gray* is a user defined function that binary code is transformed into gray code.

Step 6 : Substitute gray code value to MSB of CI. Created shared cover image (SCI), SCI = {SCI_1,

$SCI_2,\cdots,SCI_n\}$.

As LSBs in *CI* is transformed into gray code, security is also stronger than binary code that is impossible to guess which information was hided into images.

3.3 Reconstructing procedure

Fig. 2 shows the proposed decoding algorithm for reconstructing the embed secret message. There are a number of secret cover images (*SCI*) that is stored secret information. It is possible to reconstruct secret information from *SCI* by performing the following decoding algorithm.

```
Function Reconstructing (share cover image (SCI))
  Count = 1
  [Bi] = Gray2Bi ([SCI1(i,j), SCI2(i,j), SCI3(i,j) , ··· , SCIn(i,j)]);
  SI(i) = Bi[1]⊕ Bi[2]⊕,···,⊕Bi[n]
        Return M (secret messages)
  End
```

그림 2. 복원 절차
Fig. 2. Reconstructing procedure.

Step 1: Compose of a vector to collect LSB of $\{SCI_1(i,j), SCI_2(i,j),\cdots,SCI_n(i,j)\}$.

Step 2: *Gray2Bi* is transformed gray code into binary code. That is, a gray code vector is changed to binary code vector.

Step 3: Compute the following equation.

$$SI(i) = Bi[count] \oplus Bi[count+1] \oplus \cdots \oplus Bi[count+n]$$

As a result, we can reconstructing the embed secret message *M* from SI(i).

IV. Experiments

In this section, we show our experimental results. Fig. 3 shows cover images and secret image which is used our proposed secret sharing scheme. (a), (b) and (c) are cover images (*CI*). (d) is a secret message

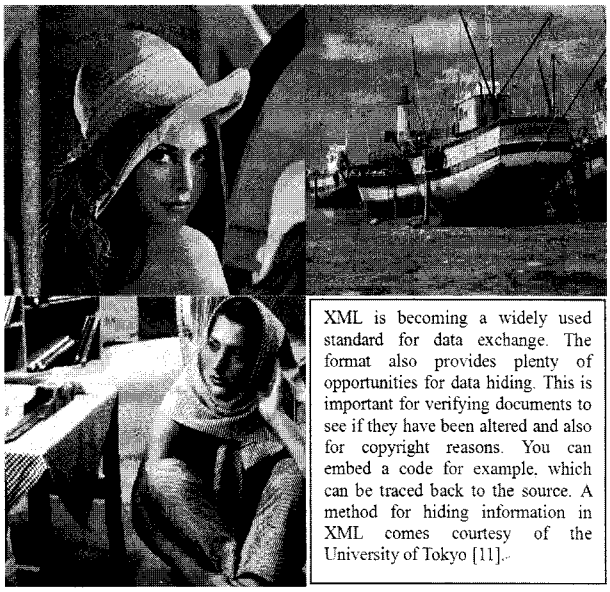


그림 3. 512 × 512크기 이미지 3개; (a), (b), (c) and (d).
Fig. 3. The image size of 512 × 512 is three images; (a), (b), (c) and (d).

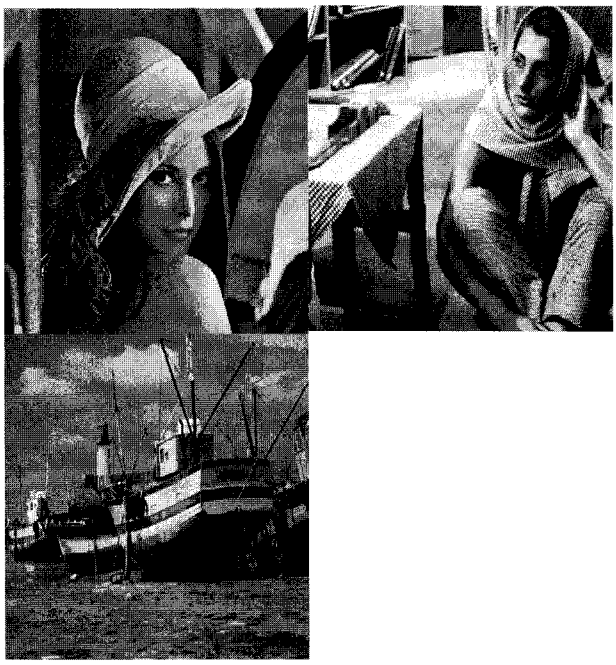


그림 4. 알고리즘 적용 후 공유 커버 이미지
Fig. 4. The result of shared cover images (SCI) 512 × 512 after embed algorithm.

(*M*). Fig. 4 is shared cover images (*SCI*) that is hided embed the secret message (*M*). Usually, steganography will be used to hide a message in an image; however, our experiment will try to hide a message in three different images. Thus, the embed message size of an image is minimized significantly.

Therefore, the proposed scheme has a good image quality at the view point of steganalysis. Fig. 4 shows the stego image that was embedding a secret message (*M*) since applying encoding algorithms in cover images. After applying our decoding algorithm on these stego images, we extract the embedded secret message (*M*) that is restored to the former state from shared cover images (*SCI*).

An original cover image (*CI*) is an image that does not embed secret information, while a shared cover image (*SCI*) is an image that does embed secret information. Therefore, an original cover image (*CI*) is different from a shared cover image (*SCI*). In our experiment, PSNR(Peek Signal To Noise Rate) is used in order to measure the difference between *CI* and *SCI*.

In our data embedding procedure, we have two primary objectives: the embed data must be imperceptible to the observer which including the observer's resources such as computer analysis, and it should have maximum payload possible. It is difficult to quantify how imperceptible embed data is. In the case of image steganography, the typical observer's detection resources include the HVS, potentially and computer analysis. Generally, in order to quantitatively evaluate, we used Mean Squared Error (*MSE*) [11] and Peak Signal to Noise Ratio (PSNR). The quality measure of *PSNR* is defined as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{I_{\max}^2}{MSE}\right) dB$$

where I_m is equal to 255 for 8 bit gray scale images. The MSE is calculated as follows:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|CI_{i,j} - SCI_{i,j}|)^2$$

M and N indicate the total number of the pixels in the horizontal and vertical dimensions of the image. $CI_{i,j}$ represent the pixels in the original image and $SCI_{i,j}$ represent the pixels of the stego-image. During the performance testing, several images taken and steganographic operation applied by the proposed scheme. As a result of Fig. 3 and Fig. 4, we get PSNR of Table 2 and it is very good result compre with DCT based scheme.

표 2. 그림 3에 대한 제안 방법의 성능
Table 2. Performance of the proposed scheme of fig.3.

Images (512x512) BMP	Size	Embed data (bit)	PSNR[dB]
Lena	512×512	6288	70.5207
Boat	512×512		70.3379
Barbara	512×512		70.3766

XML is becoming a widely used standard for data exchange. The format also provides plenty of opportunities for data hiding. This is important for verifying documents to see if they have been altered and also for copyright reasons. You can embed a code for example, which can be traced back to the source. A method for hiding information in XML comes courtesy of the University of Tokyo [11].

그림 5. 복원 알고리즘 적용 후 비밀 메시지
Fig. 5. The secret message after reconstruction algorithm.

Several 512×512 size images were chosen. Actually, proposed scheme is very simple and easy. Encoder and decoder for steganography were tested a lot of images and embed message. Sample image were 512×512 BMP scale images.

Three stego images were made from three original images and embed data by proposed algorithm. Three different aspects in information-hiding systems content with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover image, security refers to isolation to detect hidden information, and robustness refers to withstand without destruction of hidden information.

The proposed method used XOR operation and gray code. The purpose of this is that it provides enhanced security when the embed data was distributed three images. As a result, the security can

표 3. 랜덤함수로 생성한 비밀 메시지에 대한 제안 방법의 성능

Table 3. Performance of the proposed scheme with random generated secret message.

Images (512x512) BMP	Embed data	PSNR[dB] (Lin-Tsi scheme)	PSNR[dB]
Lena(512×512)	262,144 bit	38.52	51.13
Boat(512×512)		38.40	51.14
Barbara(512×512)		38.12	51.13

be increased more than any other scheme.

In another experiment, secret message was generated by random function of Matlab, its size is 262114 bits, as you can see in Table 3. The PSNR is very high in maximum size of a random secret message rather than that of Lin-Tsai scheme. Therefore, our propose scheme is imperceptible rather than any other scheme.

V. Results & Future Works

In this paper, we proposed a new secret sharing scheme for steganography. The proposed scheme can be easilt implemented by any appropriate programming languages. The most important property of the proposed scheme is that the message information is scattered at the cover image pixels of three images with regular rules. It means that the proposed scheme is simple and robust.

By evaluating the Fig. 3,4 and 5 and Tables 2 and 3, it can be seen that the proposed scheme is very practical and secure when we hide a secret information into cover images. That is, the PSNR show that the best results are achieved when the message information is hidden in more than three images because of data distribution of hidden message.

In the future, we will develop a new scheme of secret sharing method for security and ability of storing a hidden message. Moreover, a defense scheme for steganalysis should be developed for robust security in various application fields.

References

[1] Raja, K.B.; Vikas; Venugopal, K.R.; Patnaik, L.M., High Capacity Lossless Secure Image Steganography using Wavelets, International Conference on Advanced Computing and Communications, vo., Issue , 20-23 Dec. 2006 Page(s):230 - 235.

[2] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security and Privacy, vol. 1, no. 3, pp. 32-44, May, 2003.

[3] Westfeld A., and Pfitzmann A., "Attacks on steganographic systems," Lecture Notes in Computer Science, vol. 1768, pp. 61-75, 2000

[4] Fridrich J., Goljan M., and Hogea H., "Attacking the OutGuess," Proceedings of the ACM Workshop on Multimedia and Security, pp. 967-982, 2002.

[5] Sallee P., "Model-based steganography," Lecture Notes in Computer Science, vol. 2939, pp. 154-167, 2004.

[6] Westfeld A., "F5: A steganographic algorithm: High capacity despite better steganalysis," Lecture Notes in Computer Science, vol. 2137, pp. 289-302, 2001.

[7] Solanki K., Sarkar A., Manjunath B. S., "YASS: Yet another steganographic scheme that resists blind steganalysis," Proceedings of the 9th International Workshop on Information Hiding, Saint Malo, Brittany, France, pp.16-31, 2007.

[8] Thien, C.C., Lin, J.C., 2002. Secret image sharing. Computers & Graphics, 26 (1), 765 - 770.

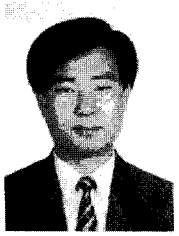
[9] Chang, C.C., Hwang, R.J., 1998. Sharing secret images using shadow codebooks. Information Sciences 111 (1 - 4), 335 - 345.

[10] Feng, J.B., Wu, H.C., Tsai, C.S., Chu, Y.P., 2005. A new multi-secret images sharing scheme using Largrange's interpolation. The Journal of Systems & Software 76 (3), 327 - 339.

[11] Shamir, A., 1979. How to share a secret. Communications of the Association for Computing Machinery, 612 - 613.

[12] Lin, C.C., Tsai, W.H., 2004. Secret image sharing with steganography and authentication. Journal of Systems & Software 73 (3), 405 - 414.

저 자 소 개



김 천 식(정회원)

1997년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
2003년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
2000년~2003년 경동대학교 정보통신공학부 교수
2004년~현재 안양대학교 교수
2007년~현재 대한전자공학회 컴퓨터소사이어티 분과위원장
2008년~현재 인터넷 방송통신 TV학회 상임이사
2006년~현재 인터넷 정보학회 학회편집위원
2006년~현재 대한교통학회 정회원
2005년~현재 한국데이터베이스학회 정회원
<주관심분야: 데이터베이스, 데이터마이닝, 유비쿼터스, 텔리매틱스, TPEG, DMB, 홈네트워크, e-Learning>

윤 은 준(정회원)

2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년~현재 경북대학교 전자전기컴퓨터학부 연구교수
2007년~현재 보안공학연구지원센터 보안공학논문지 편집위원
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>

홍 유 식(정회원)

1984년 경희대학교 전자공학과 (학사)
1989년 뉴욕공과대학교 전산학과 (석사)
1997년 경희대학교 전자공학과 (박사)
1985년~1987년 대한항공(N.Y.지점 근무)
1989년~1990년 삼성전자 종합기술원 연구원
1991년~현재 상지대학교 컴퓨터공학부 교수
2000년~현재 한국 퍼지 및 지능시스템학회 이사
2004년~현재 대한전자공학회 ITS 분과위원장
2001년~2003년 한국정보과학회 편집위원
2001년~2003년 한국컴퓨터교육산업학회 이사, 편집위원
2004년~현재 건설교통부 ITS 전문심사위원
2004년~현재 원주 시 인공지능신호등 심사위원
2005년~현재 정보처리학회 이사
2005년~현재 인터넷 정보학회 이사
2005년~현재 정보처리학회 강원지부 부회장
2006년~현재 인터넷 방송통신 TV학회 상임이사
<주관심분야: 퍼지 시스템, 전문가시스템, 신경망, 교통제어>

김 형 중(평생회원)

1978년 서울대학교 전기공학과 (공학사)
1986년 서울대학교 제어계측공학과 (공학석사)
1989년 서울대학교 제어계측공학과 (공학박사)
1992년~1993년 USC 방문교수
1989년~2006년 강원대학교 교수
2006년~현재 고려대학교 정보경영공학부 교수
<주관심분야: 멀티미디어보안, 분산처리, 콘텐츠 공학 등>