Journal of The Korea Society of Computer and Information
Vol. 19, No. 12, December 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.12.153

데이터 손상을 최소화하는 사이드 매치를 이용한 역연산 기반 이미지 스테가노그래피

최 원 석*, 정 경 호**, 김 성 수***, 윤 태 진***, 한 기 준*

Inverse Operation-based Image Steganography using Side Match for Minimum Data Damage

Won-Seok Che*, Kyung-Ho Chung**, Sung-Soo Kim***, Tae-Jin Yun***, Ki-Jun Han*

요 약

디지털 이미지에 대한 스테가노그래피 방법들은 원본 이미지의 왜곡 없이 많은 데이터들을 숨겨야 한다. 그 방법들 중 하나로써 비밀 데이터를 삽입 할 픽셀 주위에 있는 픽셀들의 평균값을 이용하여 해당 픽셀에 들어갈 비밀 데이터를 생성하여 삽입하는 기법은 삽입할 비밀 데이터가 클수록 기존 픽셀 값의 변화도 커지기 때문에 원본 이미지에 대한 손상 또한 커지게 된다. 본 논문에서는, 측면 픽셀들의 평균값에 비밀 데이터 값의 차를 이용하여 비밀 데이터를 삽입할 픽셀의 값을 연산함으로써 기존 픽셀 값과의 차이를 줄이는 기법을 제안한다. 본 기법을 적용함으로써 더 많은 비밀 데이터의 삽입이 가능하였고 이미지의 품질 손상 또한 줄일 수 있었다.

▸ Keywords : 스테가노그래피, 디지털 이미지, 사이드 매치, 보안

Abstract

The Streganography method for digital images has to insert secret data into the image without image distortion. Side match method is that size of secret data is calculated by difference of embedded pixel value and mean value of side pixels. And the secret value is embedded into the embedded pixel. Therefore, the more secret data increases, the more image distortion increases, too. In this paper, we propose the enhanced method that calculates embedded pixel value by difference of secret value and mean value of side pixels. In proposed method, more secret data is embedded and image distortion has to decreases.

▸ Keywords : Steganography, Digital image, Side match, security

•제1저자 : 최원석 •교신저자 : 한기준
•투고일 : 2014. 9. 3, 심사일 : 2014. 10. 7, 게재확정일 : 2014. 12. 1.
* 경북대학교 컴퓨터학부(Shool of Computer Science and Engineering, Kyungpook National University)
** 경운대학교 컴퓨터공학과(Department of Computer Engineering, Kyungwoon University)
*** 경운대학교 모바일공학과(Department of Mobile Engineering, Kyungwoon University)

I. 서 론

통신 기술이 발달함에 따라 관련 산업 및 연관 분야가 함께 발전하고 있으며 인간의 삶 또한 윤택해지고 있다. 그러나 통신 기술이 여러 분야에서 활용되고 있다는 것은 이에 대한 보안 위협 또한 증가하고 있다는 것을 의미한다. 그러므로 이런 보안 위험 요소를 제거하기 위한 방법이 강구되어야 한다. 암호 기법 중 DES, RSA 등의 크립토그래피는 암호 알고리즘을 이용하여 데이터를 암호화함으로써 공격자로부터 정보를 보호하는 방법이다. 한편, 스테가노그래피는 공격자가 알아채지 못하게 디지털 매체에 특정 메시지를 삽입하는 기법이다. 그 중, 디지털 이미지에 대한 스테가노그래피 기법은 원본 이미지의 유사성을 유지하고 왜곡된 이미지를 발생시키지 않으면서 많은 양의 비밀 데이터를 삽입시키는 것이 중요한 관건이다.

2004년도에 발표된 논문 [1]은 주위 픽셀들을 참조하여 edge area와 smooth area를 판단하여 edge 부분에 더 큰 비트 길이의 데이터를 삽입시키는 방식이다. 이와 관련한 개선 연구로써, 2009년 Chen과 Wu의 [4], 2013년 Swain의 [5][6]이 발표되었다. 상기 연구들은 삽입할 픽셀 값과 측면 픽셀들의 평균값의 차를 이용하여 비밀 데이터를 생성하고 삽입하기 때문에 비밀 데이터의 크기가 커질수록 원본 이미지의 손상 정도도 커질 수 밖에 없다.

본 논문에서는, 측면 픽셀들의 평균값과 비밀 데이터 값의 차를 이용하여 삽입할 픽셀 값을 결정한다. 그러므로 삽입할 픽셀의 기존 값과의 차이를 줄임으로써 원본 이미지의 손상을 줄이고 더 많은 비밀 데이터를 삽입할 수 있다.

2장에서는 기존 연구인 [1]을 서술하였고 3장에서는 본 논문의 제안 기법을 설명한다. 4장에서는 2장에서의 기존 연구와 본 제안 연구를 비교 분석하였고 5장에서 본 연구의 결론을 맺는다.

II. A steganographic method for digital images using side match

본 모델은 2004년에 Chang, Tseng이 발표한 스테가노그래피 기법 [1] 이다. 해당 기법은 비밀 데이터를 삽입할 픽셀의 주위 픽셀들을 비교하여 삽입될 비밀 데이터의 비트 수를 계산한 후 비밀 데이터의 값을 정한다. 이 비밀 데이터 값으로 특정 픽셀의 새로운 gray value를 계산한 후 기존의 값과 치환한다. 해당 논문에서 제안하는 방법 중 Two-sided side match, Four-sided side match steganography의 내용은 다음과 같다.

1) Two-sided side match steganography

첫 행과 열은 연산 대상의 픽셀들이 아니며 Raster-scan 순서로 픽셀들을 연산한다. 특정 픽셀 P_x의 gray value는 G_x, P_x의 좌측, 상단 픽셀의 gray value를 각각 G_l, G_u라고 하자.

전체적인 연산 과정은 다음과 같다.

$$d = (G_u + G_l)/2 - G_x. \tag{1}$$

$$n = \log_2|d|, \quad \text{if } |d| > 1. \tag{2}$$

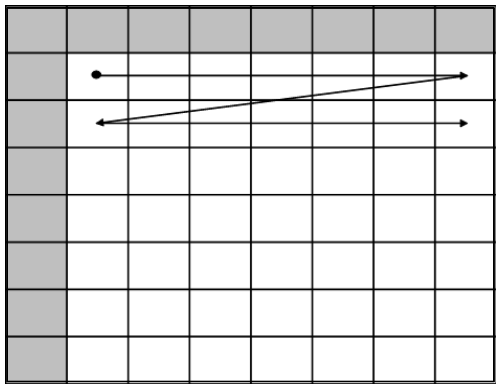


그림 1. The two-sided match steganography 에서의 raster-scan order
Fig. 1. Raster-scan order for two-sided side match steganography

(1)과정에서 difference value d를 구한 후 그 값이 1, 0, -1이면 LSB 치환 방법을 사용하여 1 비트를 치환한다. (2)과정에서 비밀 데이터의 비트 수 n을 구하고 비트 수에 맞게 비밀 데이터 값 b를 정한다.

$$d' = \begin{cases} 2^n + b, & \text{if } d > 1; \\ -(2^n + b), & \text{if } d < 1. \end{cases} \tag{3}$$

$$G_x = (G_u + G_l)/2 - d'. \tag{4}$$

(3), (4)의 연산으로 G_x는 새로운 gray value로 치환된

다. 만약 새로운 gray value가 [0, 255]의 범위를 넘는다면 그 gray value를 할당하지 않고 그 픽셀에 대하여 데이터의 삽입, 추출 연산을 하지 않는다. 비밀 데이터 추출 연산 과정은 다음과 같다.

$$d^* = (G_u^* + G_l^*)/2 - G_x^*. \tag{5}$$

$$n = \log_2|d^*|, \quad \text{if } |d^*| > 1. \tag{6}$$

$$b = \begin{cases} d^* - 2^n, & \text{if } d^* > 1; \\ -d^* - 2^n, & \text{if } d^* < 1. \end{cases} \tag{7}$$

2) Four-sided side match steganography

그림2)에 음영으로 표시된 부분은 삽입, 추출연산 대상이 아님을 나타낸다. 특정 픽셀 측면의 좌, 우, 상, 하에 대한 4개의 픽셀들을 참조한다. Two-sided side match 방식과 대부분의 연산 과정은 동일하며 다른 부분은 다음과 같다.

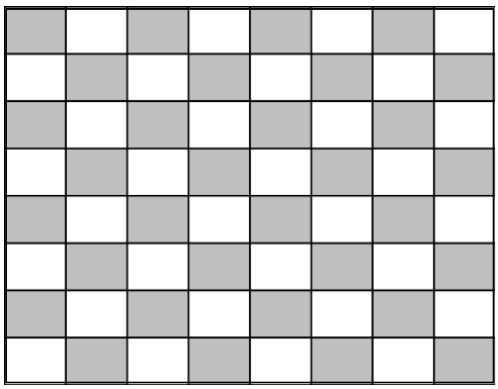


그림 2. Four-sided side match steganography에서의 픽셀 배열
Fig. 2. The pixels used for four-sided side match

$$d = (G_u + G_l + G_r + G_b)/4 - G_x. \tag{8}$$

$$G_x = (G_u + G_l + G_r + G_b)/4 - d'. \tag{9}$$

위 2가지 방법 외에, Three-sided side match steganography는 3 가지 타입으로 정의된 픽셀 배열에서 측면 픽셀 3개 또는 4개를 이용하여 비밀 데이터를 생성하여 삽입한다. 나머지 연산 방법은 동일하다.

III. 제안 기법

본 논문에서 제안하는 방법에서는 비밀 데이터 값과 측면 픽셀들의 평균값을 이용하여 비밀 데이터를 삽입할 픽셀의 값을 연산함으로써 기존 픽셀 값과의 차를 줄인다.

Two-sided side match steganography와 같은 raster-scan order 방식을 사용한다. 비밀 데이터를 삽입할 픽셀의 gray value를 G_x라고 하면 이 픽셀 측면의 좌측, 좌측 상단, 상단, 우측 상단 픽셀들의 gray value는 각각 G_l, G_{lu}, G_u, G_{ru}으로 표현한다.

각 픽셀에 들어갈 비밀 데이터의 비트 수를 구하기 위해 연산을 할 때 G_l, G_{lu}, G_u, G_{ru}를 참조하며 그림 3에서 볼 수 있듯이 우측 상단 값, G_{ru}를 참조할 수 없는 경우는 G_{ru}를

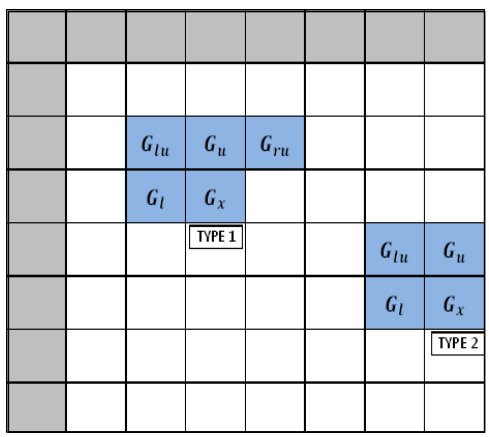


그림 3. 제안 기법의 TYPE1, TYPE2에 대한 픽셀 배열
Fig. 3. Proposed method

생략하고 그 외의 3개 픽셀들을 참조한다.

전체적인 연산 과정은 다음과 같다.

$$d = \begin{cases} (G_l + G_{lu} + G_u + G_{ru})/4 - G_x, \\ \quad \text{if } \exists\, G_{ru}; \\ (G_l + G_{lu} + G_u)/3 - G_x, \\ \quad \text{if } \exists!\, G_{ru}. \end{cases} \tag{10}$$

$$n = \log_2|d|, \quad \text{if } |d| > 1. \tag{11}$$

$$SV = \begin{cases} b, & \text{if } d > 1; \\ b \times -1, & \text{if } d < 1. \end{cases} \quad (12)$$

수식 10은 G_l, G_{lu}, G_u, G_{ru}의 평균값에서 G_x를 뺀 값, d,를 구하는 수식이다. G_{ru}가 존재하지 않는다면 이를 제외시킨 평균값을 이용한다. 수식 11의 연산을 이용하여 n을 구하고 n-bit의 범위 내에서 비밀 데이터 b를 생성한다. $|d|$가 1보다 작다면 LSB 치환 방법을 사용하여 1비트를 치환한다. 수식 12에서, b의 값을 SV로 할당하고 만약 d가 1보다 작으면 b의 값에 -1을 곱하여 SV에 할당한다.

$$G_x = \begin{cases} (G_l + G_{lu} + G_u + G_{ru})/4 - SV, \\ \quad \text{if } \exists\, G_{ru}\,; \\ (G_l + G_{lu} + G_u)/3 - SV, \\ \quad \text{if } \exists!\, G_{ru}\,. \end{cases} \quad (13)$$

수식 13은 주위 픽셀들의 평균값에서 SV를 뺀 값을 이용하여 G_x에 대입함으로써 새로운 픽셀 값을 할당함을 나타낸다.

$$SV = \begin{cases} (G_l^* + G_{lu}^* + G_u^* + G_{ru}^*)/4 - G_x^*, \\ \quad \text{if } \exists\, G_{ru}^*\,; \\ (G_l^* + G_{lu}^* + G_u^*)/3 - G_x^*, \\ \quad \text{if } \exists!\, G_{ru}^*\,. \end{cases} \quad (14)$$

$$b = |SV| \quad (15)$$

비밀 데이터를 추출하는 연산을 살펴보자. 수식 14는 SV를 구하는 연산으로써 주위 픽셀들의 평균값에서 비밀 데이터를 추출한 픽셀 G_x^*의 값을 빼 SV를 구한다. 비밀 데이터 b는 SV의 절대값이다.

IV. 실험 결과

제안 기법과의 비교 기법은 삽입 픽셀 수가 동일한 "A steganographic method for digital image using side match"기법 중 two-sided side match이다. 4개의 비트맵 파일을 이용하여 PSNR과 Capacity를 비교하였다. 본 논문의 실험에서는 512*512*256 비트맵 파일이 사용되었고 비밀 데이터는 임의의 비트열을 사용하였다. 비교 결과는 표 1과 같다.

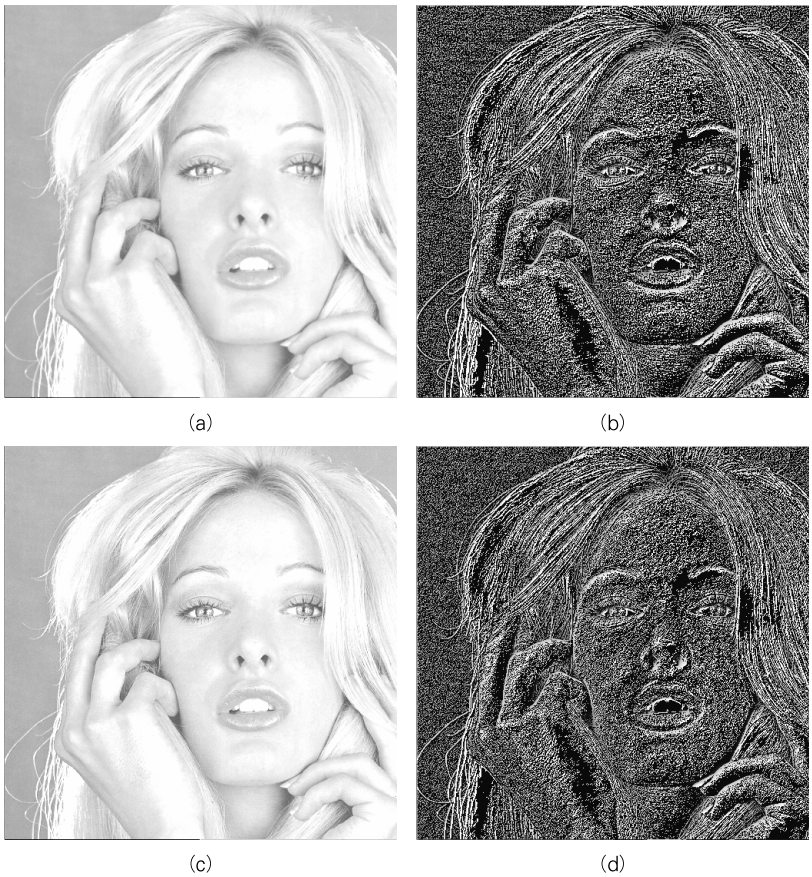
3개의 이미지 파일, Tiffany, Baboon, F16에서는 제안 기법이 비교 기법보다 PSNR 값이 높음에도 불구하고 Capacity가 더 큼을 확인할 수 있다. Lena 이미지 비교에서는, 제안 기법의 PSNR이 1.95 크고 capacity는 356이 작은 일반적인 비례 관계를 나타낸다.

기존 기법과 비교하여, 제안 기법에 의하여 Tiffany 이미지에서는 PSNR은 3.7%, capacity는 3.5%, Baboon 이미지에서는 PSNR은 10%, capacity는 3.4%, F16 이미지는 PSNR이 6.3%, capacity는 4.6%가 향상됨을 확인할 수 있다.

그림 4, 5, 6은 제안 기법과 기존 기법으로 처리된 이미지와 삽입된 비밀 데이터를 표시한 이미지를 나타낸다. 제안 기법에 의한 비밀 데이터 삽입량이 더 많기 때문에 비밀 데이터 이미지에서 밝은 부분이 더 많이 표시되어 있음을 확인할 수 있다.

표 1. PSNR과 비밀 데이터를 숨길 수 있는 비트 수의 총량을 나타내는 Capacity 측정 결과
Table 1. PSNR and capacity comparison

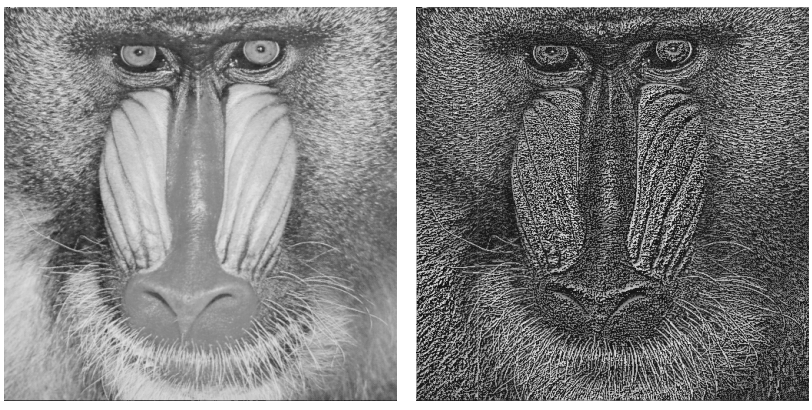
	Two-sided side match		Proposed	
	PSNR	Capacity	PSNR	Capacity
Tiffany	36.71	415867	38.08	430688
Baboon	27.83	722630	30.62	747339
F16	34.95	404692	37.18	423658
Lena	37.76	386417	39.71	386061



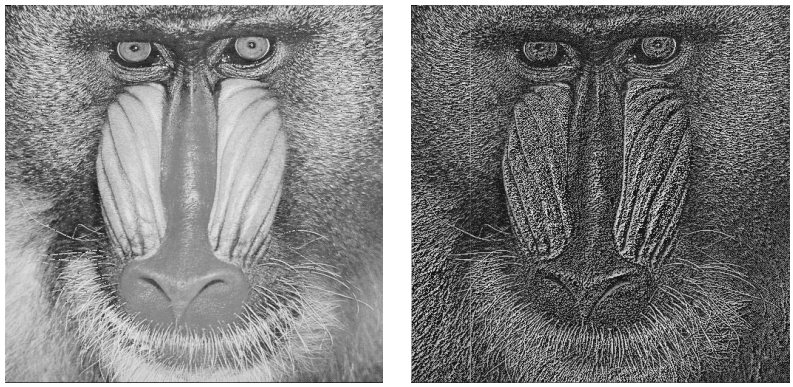
(a) (b)

(c) (d)

그림 4. (a) 제안 기법에 의한 이미지, (b) 제안 기법에 의한 비밀 데이터 표시 이미지
(c) Two-sided side match에 의한 이미지, (d) Two-sided side match에 의한 비밀 데이터 표시 이미지
Fig. 4. (a) The image by proposed method, (b) Secret data image by proposed method
(c) The image by two-sided side match, (d) Secret data image by two-sided side match

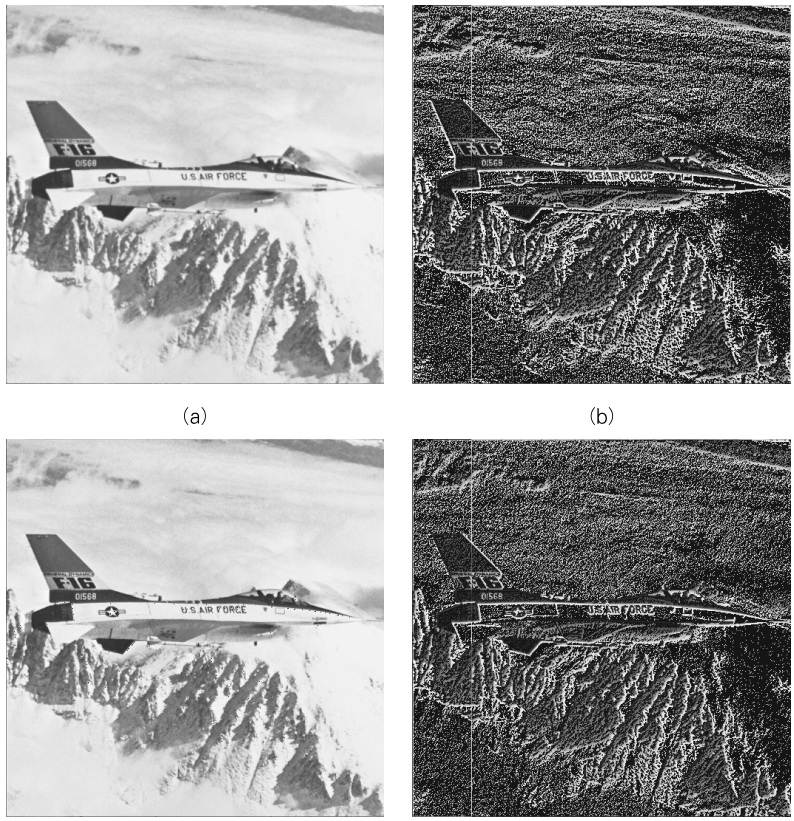


(a) (b)



(c) (d)

그림 5. (a) 제안 기법에 의한 이미지, (b) 제안 기법에 의한 비밀 데이터 표시 이미지
(c) Two-sided side match에 의한 이미지, (d) Two-sided side match에 의한 비밀 데이터 표시 이미지
Fig. 5. (a) The image by proposed method, (b) Secret data image by proposed method
(c) The image by two-sided side match, (d) Secret data image by two-sided side match



(a) (b)

(c) (d)

그림 6. (a) 제안 기법에 의한 이미지, (b) 제안 기법에 의한 비밀 데이터 표시 이미지
(c) Two-sided side match에 의한 이미지, (d) Two-sided side match에 의한 비밀 데이터 표시 이미지
Fig. 6. (a) The image by proposed method, (b) Secret data image by proposed method
(c) The image by two-sided side match, (d) Secret data image by two-sided side match

V. 결 론

스테가노그래피 기법 중 사이드 매치를 이용한 픽셀 값의 차를 이용한 기존 기법은 비밀 데이터를 삽입하는 방식이기 때문에 그 값이 커질수록 원본 데이터 손상도도 증가한다.

본 논문에서 제안한 방법은 기존 연구들에서 사용하던 삽입 픽셀에 비밀 데이터를 추가하는 방법을 탈피하여 측면 픽셀들의 평균값과 비밀 데이터의 차의 값을 삽입 픽셀 값으로 치환하는 방식으로 이미지 손상을 줄이는 방식을 채택하였다. 이 기법은 원본 픽셀 값에 근접한 치환 값을 연산하기 때문에 본 제안 기법을 적용함으로써 원본 이미지의 손상을 줄이면서도 더 많은 비밀 데이터를 삽입할 수 있음을 실험 결과로 확인할 수 있었다. 앞으로의 연구에서 비밀 데이터 삽입 비율을 높이고 동시에 원본 데이터 손상도를 더욱 줄일 수 있는 방법을 연구할 계획이다.

Acknowledgement

이 논문은 2012년도 경북대학교 학술연구에 의하여 연구되었음.

참고문헌

〔1〕 C.C.Chang and H.W.Tseng, "A Steganographic Method for Digital Images using Side Match," Pattern Recognition Letters, Vol. 25, Issue 12, pp. 1431-1437, September 2004.

〔2〕 C.C.Chang, C.Y.Lin and Y.Z.Wang, "New Image Steganographic Methods using Run-length Approach," INFORMATION SCIENCES, February 2006.

〔3〕 A. Martin, G. Sapiro and G. Seroussi, "Is Image Steganography Natural?," IEEE TRANSACTIONS ON IMAGE PROCESSING, Vol. 14, No. 12, December 2005.

〔4〕 P. Chen, W. Wu, "A Modified Side Match Scheme for Image Steganography," International Jounal of Applied Science and Engineering, Vol. 7(1), pp. 53-60, October 2009.

〔5〕 G. Swain, S. K. Lenka, "Steganography using two sided, three sided, and four sided side match methods," CSI Transactions on ICT, Vol. 1, Issue 2, pp. 127-133, June 2013.

〔6〕 G. Swain, "Steganography in Digital Images Using Maximum Difference of Neighboring Pixel Values," International Journal of Security and Its Applications, Vol. 7, No. 6, pp. 285-294, 2013.

〔7〕 M. A. B. Younis, and A. Jantan, "A New Steganography Approach for Image Encryption Exchange by Using Least Significant Bit Insertion," International Journal of Computer Science and Network Security, Vol. 8, No. 6, 2008.

〔8〕 M. Juneja, P. S. Sandhu, and E. Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images," Proceedings of World Academy of Science, Engineering and Technology, Vol. 38, pp. 427-429, 2009.

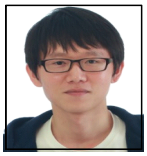
〔9〕 M. Amiri, and M. R. Resketi, "An Edge Method in Steganography," Proceedings of World Academy of Science, Engineering and Technology, Vol. 37, pp. 1058-1063, 2009.

〔10〕 S. Arora, and S. Anand, "A New Approach for Image Steganography using Edge Detection Method," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 3, May 2013.

〔11〕 G. Yim, and H. Kim, "Chaos-based Image Encryption Scheme using Noise-induced Synchronization," Journal of the Korea Society of Computer and Information, Vol. 13, No. 5, pp. 155-162, September 2008.

〔12〕 H. Yang, and J. Choi, "Study on the Correlation between Digital Images using ICOR," Journal of the Korea Society of Computer and Information, Vol. 14, No. 3, pp. 75-82, March 2009.

저 자 소 개



최 원 석

2007: 안동대학교
컴퓨터공학과 학사
2011: 경북대학교
전자전기컴퓨터학부 석사
현 재: 경북대학교
컴퓨터학부 박사 과정
관심분야: Security, 임베디드 시스템
Email : theenemys@knu.ac.kr

정 경 호

2000: 대구대학교
컴퓨터정보공학과 학사
2002: 경북대학교
컴퓨터공학과 석사
2011: 경북대학교
컴퓨터공학과 박사
현 재: 경운대학교
컴퓨터공학과 조교수
관심분야: 임베디드 시스템, 정보보호
Email : mccart@ikw.ac.kr

김 성 수

2002: 금오공과대학교
컴퓨터공학과 학사
2005: 경북대학교
컴퓨터공학과 석사
2012: 경북대학교
컴퓨터공학과 박사
현 재: 경운대학교
모바일공학과 조교수
관심분야: 임베디드 시스템, RFID
Email : ninny@ikw.ac.kr

윤 태 진

1994: 경북대학교
컴퓨터공학과 학사
1996: 경북대학교
컴퓨터공학과 석사
2012: 경북대학교
컴퓨터공학과 박사
현 재: 경운대학교
모바일공학과 부교수
관심분야: 임베디드 시스템, 정보보안
Email : tjyun@ikw.ac.kr

한 기 준

1979: 서울대학교
전기공학과 학사
1981: KAIST
전기 및 전자공학과 석사
1985: University of Arizona
Dept. of ECE (M.S.)
1987: University of Arizona
Dept. of ECE (Ph.D.)
현 재: 경북대학교
컴퓨터학부 교수
관심분야: 무선 네트워크
Email : kjhan@knu.ac.kr