Available online at www.elixirpublishers.com (Elixir International Journal)

Digital Processing

Elixir Digital Processing 82 (2015) 32105-32107

ISSN: 2229-712X

Image Hiding using Range Normalization

B. Lakshmi Sirisha, S. Srinivas Kumar and B. Chandra Mohan
Department of ECE, Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India.

ARTICLE INFO

Article history:
Received: 26 February 2015;
Received in revised form:
19 April 2015;
Accepted: 30 April 2015;

Keywords
Data Hiding,
Image Hiding,
Range Normalization,
Steganography,
Secret Image Sharing.

ABSTRACT
This paper proposes an image hiding technique that exhibits good quality with higher embedding capacity. In this technique, both secret and cover images are divided into non overlapping blocks. The secret image is embedded into a cover image block by block using Range Normalization Technique. This technique exhibits advantages of high embedding capacity with less computational complexity. Compared with the existing algorithms, the quality of the stego and reconstructed image is found to be good.

Introduction

The basic idea of image hiding is, to hide the message (secret) under the camouflage of the cover image. Mixing of secret and cover images is called a stego-image. Both the stego and cover images are visually indistinguishable, so that an unintended observer will not be able to notice the existence of secret image.

Most of the data hiding techniques [1-4], based on manipulating the Least Square Bits (LSB) by directly replacing the LSB bits of the cover image with the message bits. Due to the limited number of LSB bits in a cover image, these techniques often works well when the size of the message is small. When the embedding message is large, the quality of stego image is found to get degraded. In order to achieve a high embedding capacity with acceptable stego quality, Lin and Tsai [5] proposed a secret image sharing method that is based on the lossy polynomial image sharing, but the image reconstructed in this method is found to be distorted. Wu et al., [6] proposed a sharing and hiding method based on modulus operation. By this method, the secret image cannot be retrieved completely.

Thien and Lin [7], Chang et al., [8], Zhao et al.,[9] used two pixels to represent the gray values larger than 250 for recovering the secret image. Though these are effective, the stego images are random in nature which attracts the attention of malicious attackers. Chang et al., [8], Zhao et al., [9], Yang et al.,[10] and Lin et al., [10] schemes suffer from the expansion of secret image and may reduce the capacity of the embedded secret data and distort the quality of stego image.

Inspired by potential practicability, Pei-Yu Lin et al., [12] proposed an invertible sharing scheme with steganography to recover the lossless secret and cover images. Their scheme is worthwhile, but the computation cost to reconstruct the secret and cover images is relatively high since Lagrange interpolation is used. Moreover, parameter k must be a prime number, which makes it not so flexible.

In the proposed scheme, the secret pixels mapped to cover pixels based on well-known technique called Range Normalization, so that a stego image is formed. Proposed scheme is a simple with low computational cost and reconstructs the secret and cover images with a good quality.

Proposed Method

Secret image and cover image of the same size are considered in the proposed method. Gray level values of the secret image are transformed into the gray level values of cover image block by block using Range Normalization Technique and on transformation, a stego image is formed.

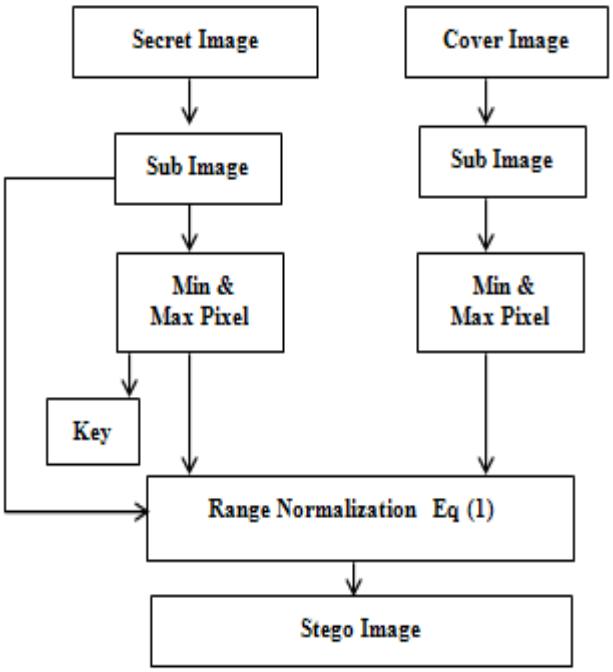

Figure 1. Flowchart of embedding scheme

Embedding procedure

The flow chart of embedding scheme is shown in Fig 1. Let R and S be the cover image of size $M_R \times N_R$ and secret image of size $M_S \times N_S$ respectively. Both secret and cover images are divided into non overlapping blocks of size $I \times J$.

Tele:
E-mail addresses: suravarapuls@gmail.com

Table 1. Image qualities of stego image

Stego image	MSE	PSNR	SSIM	LMSE	NAE
aero plane	2.89248	33.5181	0.9952	0.7180	0.0214
barb	3.00009	33.3595	0.9977	0.7143	0.0219
bridge	3.29016	32.9586	0.9937	0.7309	0.0234
cat	3.29559	32.9515	0.9971	0.7404	0.0235
crane	3.26335	32.9942	0.9976	0.7326	0.0236
house	2.83403	33.6068	0.9975	0.7037	0.0216
lena	2.80715	33.6481	0.9988	0.7085	0.0212
people	3.00705	33.3494	0.9970	0.7087	0.0221

Table 2. Comparison of secret hiding schemes

Schemes	Features				
	Meaningful Stego Image	Lossless Cover Image	Lossless Secret Image	Extra Storage	Maximum Embedding Capacity
Thien and Lin (2002)	N/A	N/A	Yes	Yes	N/A
Wu et al., (2004)	Yes	No	No	No	N/A
Lin and Tsai (2004)	Yes	No	No	No	$MXN/4$
Yang et al.,(2007)	Yes	No	Yes	No	$M*N/4$
Chang et al., (2008)	Yes	No	Yes	Yes	$M*N/4$
Zhao et al., (2009)	No	Yes	Yes	Yes	N/A
Lin et al., (2009)	Yes	N/A	Yes	No	$t-3*M*N/4$
Pei-Yu Lin et al.,(2010)	Yes	Yes	Yes	No	$t-1*M*N/\log_{10}(256)$
Proposed scheme	Yes	Yes	Yes	No	$t*M*N/\log_{10}(256)$

The secret image is embedded into cover image in a block by block sequence using Range Normalization Technique as

$$G_i(I,J)=\left[\frac{Max(R_i)-Min(R_i)}{Max(S_i)-Min(S_i)}\right]*(S_i(I,J)-Min(S_i))+Min(R_i) \quad (1)$$

Where R_i and S_i represent the i^{th} block of R and S respectively. Each pixel of the i^{th} block of the stego image is represented as $G_i(I,J)$. $Max(R_i)$ and $Min(R_i)$ represents the maximum and minimum value of i^{th} block of the cover image. $Max(S_i)$ and $Min(S_i)$ represents the maximum and minimum value of i^{th} block of the secret image. The minimum and maximum pixel values in each block of secret image are chosen as keys for lossless reconstruction.

Retrieval procedure

In *Fig*.2 , all the cover images used in the simulation and the secret image are shown.

Figure 2. Cover and secret images

The secret image is retrieved from the stego image (G) and key (K) by using De-normalization technique as,

$$T_i(I,J)=[\frac{Max(K_i)-Min(K_i)}{Max(G_i)-Min(G_i)}]*(G_i(I,J)-Min(G_i))+Min(K_i) \quad (2)$$

where G_i and K_i are the i^{th} block of stego image and keys respectively. Each pixel of the i^{th} block of the reconstructed secret image is represented as $T_{i(I,J)}$. Finally, the secret image can be reconstructed by extracting all the secret blocks as shown in the *Fig*.3

Figure 3. Result images

Result Analysis

In the proposed method of steganography, the quality and visual perception of the stego images are the main considerations. *Table*.1lists the qualities of the stego images with various cover images. Performance of the proposed scheme for various cover images considering 'Girl' as secret image is presented here. One measure often used to assess the quality of the stego image is *PSNR*(Peak Signal to Noise Ratio) as given by

$$PSNR=10\log_{10}[255/MSE]^2 dB \quad (3)$$

Where MSE is the Mean Square Error between cover image and stego image, is calculated

$$MSE=1/(M*N)\sum(R_{ij}-G_{ij})^2 \quad (4)$$

R_{ij} and G_{ij} are the pixel values of cover and stego images respectively. The Structural SIMilarity ($SSIM$) index is a method for measuring the similarity between cover and stego images and is given as

$$SSIM(x,y)=(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)/(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2) \quad (5)$$

where, μ_x,μ_y are averages and σ_x,σ_y are variances of cover and stego images respectively. $c_1=(K_1L)^2$, $c_2=(K_2L)^2$ L is

the dynamic range of the pixel values (0-255 for 8-bit gray scale images), and $K_1, K_2 << 1$ is a small constant.

Other performance measures often used to assess the quality of stego images are Laplacian Mean Square Error ($LMSE$) and Normalized Absolute Error (NAE). The smaller the values of, $LMSE$ and NAE indicates better the image quality. These measures are provided in *Table.*1Lin et al., [11] embedded $t-3$ secret digits in the cover image. Pei-Yu Lin et al., [12], have shown an improvement over [11] by embedding $t-1$ secret digits. In the proposed work, t secret digits are embedded in the cover image, clearly showing an improvement in the embedding capacity.

The comparisons of proposed scheme with existing schemes are shown in *Table.*2 .Pei-Yu Lin et al., [12] used Lagrange interpolation method for the reconstruction of cover and secret images. Lagrange interpolation method requires many computations hence computational cost is high.

Though Lagrange's formula is simple and easy to remember, its application is not speedy. It also requires close attention to sign and there is always a chance of committing some errors due to a number of positive and negative signs in the numerator and the denominator. This problem does not occur in the proposed method as it uses as simple Range Normalization Technique. Moreover, compared to Pei-Yu Lin *et al.*,[12] the proposed technique is not affected by either overflow or underflow problems.

Highlights of the proposed method

- Low Computational cost in the encryption and decryption.
- The authorized users only can easily classify their shares.
- The embedding capacity of the proposed method is higher than the existing methods shown in Table 2.
- The proposed method can recover the secret and cover images without any loss of information and does not use extra storage.

Conclusions

In this paper, a novel secret image hiding technique with reversible steganography is presented. A common drawback of image hiding technique using steganographic approaches is that, the revealed secret image is distorted because of the truncation of gray scale secret image. Although the distortion is small, it is unacceptable for significant secret content. Here, a novel hiding technique is proposed that can reveal the lossless secret image and satisfy related sharing essentials. Moreover, the reversible scheme offers large embedding capacity compared with camouflage sharing schemes. The reversibility property of the proposed hiding scheme is a practical solution for preserving valuable cover images, such as military and medical images.

References

[1] Celik M.U, Sharma.G, TekalpA.M, SaberE, "Lossless Generalized-LSB Data Embeddin", IEEE Transactions on Image Processing, 14 (2005)

[2] Chan C.K, Cheng L.M., "Hiding Data In Images By Simple LSB Substitution", Pattern Recognition, 37 (2004), pp. 469–474

[3] Lee C.F, Chen H.L, "A Novel Data Hiding Scheme Based On Modulus Function", Journal of Systems and Software, 83 (2010), pp. 832–843.

[4] Iuon-Chang Lin, Yang-Bin Lin, Chung-Ming Wang, "Hiding Data In Spatial Domain Images With Distortion Tolerance", Computer Standards & Interfaces 31(6) (2009) 1143-1149.

[5] Lin C.C., Tsai W.H., "Secret Image Sharing With Steganography And Authentication", journal of Systems and Software, 73 (3) (2004), pp. 405–414

[6] Wu Y.S., Thien C.C., Lin J.C., "Sharing and Hiding Secret Images With Size Constraint", Pattern Recognition, 37 (7) (2004), pp. 1377–1385

[7] Thien C.C., Lin J.C., "Secret Image Sharing", Computers& Graphics, Vol. 26, pp.765-770, 2002.

[8] Chang C.C., Hsieh Y.P., Lin C.H., "Sharing Secrets In Stego Images With Authentication", Pattern Recognition, 41 (10) (2008), pp. 3130–3137.

[9] Zhao R., Zhao J.J., Dai F., Zhao F.Q., "A New Image Secret Sharing Scheme To Identify Cheaters",Computer Standard Interface, 31 (1) (2009).

[10] Yang C.N., Chen T.S, Yu K.H., Wang C.C., "Improvements of Image Sharing with Steganography and Authentication", Journal of systems and software 80 (7) (2007), pp. 1070–1076.

[11] Lin P Y, Lee J S, Chang C C., "Distortion – Free Secret Image Sharing Mechanism Using Modulus Operator", pattern recognition 42 (5) 2009 , 886-895.

[12] Pei-Yu Lin, Chi-Shiang Chan, "Invertible Secret Image Sharing With Steganography", Pattern Recognition Letters. Volume 31, Issue 13, 1 October 2010, pp1887–189.