ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol.3, Issue, 6, pp.134-138, June, 2011

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEW ARTICLE

Image steganography using mod-4 embedding algorithm based on image contrast

Pramitha, K., Padma Suresh, L., and Shunmuganathan, K.L.

[1]Department of Electrical and Electronics Engineering, Noorul Islam University, Kanyakumari District, Tamilnadu State, India- 629 160

[2]Department of Computer Science Engineering, RMK Engineering College, Tiruvallur District, Tamilnadu State, India- 601 206

ARTICLE INFO

Article History:
Received 21st February, 2011
Received in revised form
15th March, 2011
Accepted 9th May, 2011
Published online 2nd June 2011

Key words:
Adaptive steganography;
Image contrast;
Mod-4 embedding.

ABSTRACT

In order to improve the capacity of the hidden secret data and to provide an imperceptible stego image quality, a new image steganography method based on image contrast is presented. A group of 2×2 blocks of non-overlapping spatially adjacent pixels is selected as the valid block for embedding the secret message. The modulo 4 arithmetic operation is further applied to all the valid blocks to embed a pair of binary bits using the shortest route modification scheme. Each secret message is also encrypted by RSA encryption algorithm to provide the system with more security. Data will be embedded inside the image using the pixels. Then the pixels of stego image can then be accessed back in order to retrieve back the hidden data inside the image. However, a secret key is needed by the receiver in order to retrieve back the data. This secret key is generated using the RSA decryption algorithm. By using the secret key to retrieve the data, it maintains privacy, confidentiality and accuracy of the data. The proposed method was tested on different gray scale images. From the experimental results, compared with the some well-known adaptive and non-adaptive steganography algorithms, the proposed method provides larger embedding capacity, while being less detectable by steganalysis methods.

INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information. Adaptive steganography with a high embedding capacity and a low distortion is an attractive topic in the area of information hiding (Yang *et al.,* 2008). In digital images, parts with high contrast and noise-like textures have been found to be appropriate locations to hide pseudo-random encrypted messages, due to the statistical similarities between the covert and the selected cover signals (Dulce *et al.,* 2007).

***Corresponding author:** pramitha2007@gmail.com

Various steganalysis attacks have been proposed in the literature to distinguish between original and stego objects. A successful attack is supposed to detect the changes in the cover objects caused by the message embedding process. Recently, a set of steganographic algorithms have been developed which employ some adaptation techniques to minimize the changes made to the cover object characteristics (Franz *et al.,* 2004). Early proposals are steganographic method which uses the difference value between two neighbor pixels to determine the number of secret bits to be embedded (Wu *et al.,* 2003) dithering to get image information that can be used by adaptive steganographic algorithms, the "pixel-value differencing" (PVD) and LSB replacement method (Wu *et al.,* 2005), the defining of texture in order to detect regions with textures not homogeneous and also an adaptive LSB steganographic method with larger embedding capacity using PVD (Franz *et al.,* 2004). In this work we propose an algorithm which selects 2×2 blocks of high contrast image parts. Message bits are embedded into these selected blocks with Mod-4 (Qi *et al.,* 2005) embedding method in order to decrease the effects of modifications caused by the embedding process. The embedding capacity denotes the number of bits that can be embedded into the given cover image. Our method can embed a large number of secret data and maintain original quality of the stego images.

Adaptive Steganography

Adaptive steganographic techniques have become a standard direction taken when striving to complicate the detection of secret communication. The consideration of cover image features when embedding information is an effort to insert digital media while keeping the visual and the statistical properties of the cover image intact. There are several such embedding methods in existence today, applicable for different formats of images and with contrasting approaches. An adaptive image steganographic model is proposed here that is based on mod-4 embedding algorithm to maximize the embedding capacity while maintaining image fidelity. We use 4 pixels to represent two bit of the message. The steganographic algorithms use a key, cover data and the embedding function to determine the position of the message into the image. In order to achieve an adaptive steganographic algorithm, we consider the following features of the embedding function:

- Pixel selection for embedding the data
- The bit representation of the message
- Modification of the cover data

To select the areas with greater diversity of grayscale level, they analyze the grayscale space distribution of regions and proposed the ConText algorithm.

Proposed Methods

A. Proposed method for Encryption

In this section we propose a RSA public key encryption for encrypting the secret message before embedded into cover image. RSA can be used for both encryption and decryption. In public key encryption the sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public key encryption is the most secure type of steganography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message. The basic algorithm as follows.

Cipher text $C = M^e \bmod n$;
Plain text $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$;

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e,n} and a private key of PR = {d,n}.

B. Proposed method for Data Hiding

In this section we propose a mod-4 embedding method for information hiding within the spatial domain of any gray scale image. This method can be considered as the improved version of (Dulce *et al.,* 2007). The input messages can be in any digital form, and are often treated as a bit stream. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the valid blocks in an image. Before embedding a checking has been done to find out whether the selected embedding pixels lies at the boundary of the image or not. Data embedding are done by mapping each two bits of the secret message in each of the valid block based on some features of that pixel. Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operations has been carried out to get back the original information.

C. Proposed Data Hiding Model

Fig.1 shows the block diagram of the proposed image steganographic model. The input messages can be in any digital form, and are often treated as a bit stream. The input message is first converted into encrypted form through proposed encryption method. This encrypted message generates the secret key which may be used as a password before starting of the embedding or extracting operation for increasing another level of security. Second the image is reshaped to the 2×2 blocks of non-overlapping spatially adjacent pixels. Then the valid blocks are selected from these blocks. Block Q is valid if the average difference between the gray level values of the pixels of that and it's mean (C) exceeds a threshold (minimum contrast), as described in (1). By definition, a valid block is associated with part of noisy region in the image.

$$\text{valid blocks(Q)} : \mathrm{C} = \left(\frac{1}{4} \sum_{x \varepsilon Q} | x - m_Q |\right) > T \qquad (1)$$

where m_Q is the mean gray level value of the pixels in the block and T is the minimum contrast defined by the user. Taken T = 10, in this work. Before describing the embedding phase, some of the variables are defined. Given a block Q,

$$\sigma_Q = \sum_{x \varepsilon Q} x$$
$$\delta(\sigma_Q, 4) = (\sigma_Q \bmod 4)_2$$
$$A = \{x \mid x \varepsilon Q, x \geq m_Q\}$$
$$B = \{x \mid x \varepsilon Q, x < m_Q\}$$

The subscript 2 in the definition of $\delta(\sigma_Q,4)$ indicates to convert the resulting value into the binary representation. It is obvious that the range of $\delta(\sigma_Q,4)$ is { 00; 01; 10; 11}.

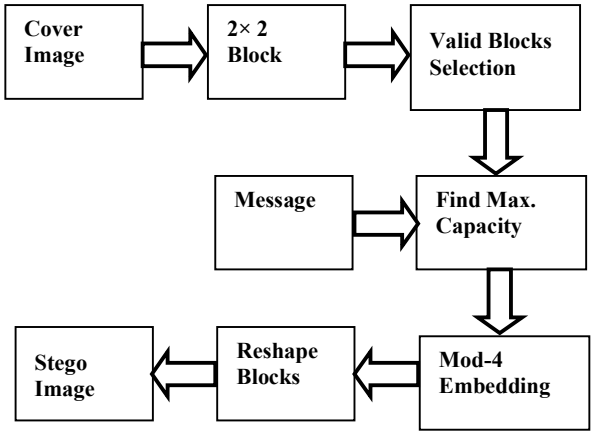

Figure 1. Block diagram for the proposed system.

Mod-4 embedding is used for embedding two bits of the message in a valid block Q with the following rules:

- Pixels with larger difference with m_Q are modified first.
- The value of C is always increased.
- The shortest route scheme is used to minimize the number of modifications for embedding each bit.

Table 1: Modification Scheme – Shortest Route

$\delta(\sigma,4)$	*p*	*n*	*Route*	*Shortest*
0	0	0	No change	N/A
1	3	1	-1 or +3	-1
2	2	2	+2 or -2	*
3	1	3	-3 or +1	+1

The shortest-route scheme is demonstrated in Table 1 where the pair of message bits to be embedded is 00. The extensions to 01, 10, and 11 could be easily derived. Let Q be the valid block under consideration. In Table 1, p column indicates the value that should be added to the pixels with values greater than m_Q. The n column is defined similarly. The last column indicates the shortest route, which uses the least number of modifications to get $\delta(\sigma_Q,4)=00$. We further define $p=\{x \mid x\varepsilon Q, x>1\}$ and $n=\{x \mid x\varepsilon Q, x<-1\}$ column is defined. The positive coefficients in Q are sorted in a decreasing order and labeled by p_1, p_2, p_3, and p_4 if $|p|=4$. On the contrary, the negative coefficients are sorted in an ascending order and labeled by n_1, n_2, n_3 and n_4. For the case that p=n=2, the number of the pixels belonging to A and B are considered.

The message bits are embedded in the set of larger numbers. To avoid embedding the message bits in pixels with critical gray level values (gray values that may exceed 256 or becomes lower than zero), the shortest route scheme is not exploited in these cases. Besides, in the embedding process, ignored blocks are inappropriate for embedding message bits due to their gray level values. Once the message is hidden inside the image, this message can be extracted back from the stego image. The extraction process is similar to the embedding process.

D. The extraction scheme

The extraction process can be carried out by reversing the embedding procedure and the block diagram is shown in Fig.2. The stego image is partitioned into non-overlapping blocks with two consecutive pixels, and the process of extracting the embedded message is the same as the embedding process with the same traversing order of blocks. The extracting process will be finished when all the bits of every bytes of secret message are extracted. Then the embedded message is retrieved from the extracted bit using the RSA decryption algorithm.

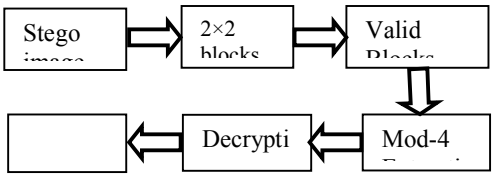

Figure 2. Block diagram for the data extraction

Experimental results

This section presents the obtained results via different processes mentioned in the proposed model. A result of the proposed data hiding method has been shown based on two benchmarks techniques. First one is the capacity of hiding data and another one is the imperceptibility of the stego image, also called the quality of stego image. The quality of stego image should be acceptable by human eyes. A comparative study of the proposed steganography methods with the existing methods like condith and the proposed methods has been shown by computing embedding capacity, mean square error (MSE) and peak signal-to noise ratio (PSNR). 829 BMP grayscale images of size approximately 256×256 pixels are used in this section to illustrate the effectiveness. The GUI design of the proposed model is shown in Fig.3.

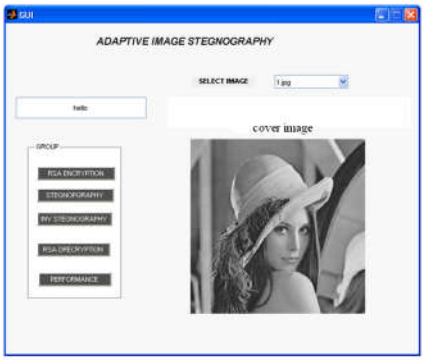

Figure 3. GUI of the proposed model

Peak Signal to Noise Ratio (PSNR)

PSNR measures the quality of the image by comparing the original image or cover image with the stego image, i.e.it measures the percentage of the stego data to the image percentage. The PSNR is used to evaluate the quality of the stego image after embedding the secret message in the cover. Assume a cover image C(i,j) that contains N by N pixels and a stego image S(i,j) where S is generated by embedding / mapping the message bit stream. Mean squared error (MSE) of the stego image as follows:

$$\text{MSE}=\frac{1}{[N\times N]^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[C(i,j)-S(i,j)]^2 \qquad (3)$$

The PSNR is computed using the following formulae:

$$\text{PSNR}=10\log_{10}255^2/\text{MSE db} \qquad (4)$$

Table 2. Contains the PSNR values for four stego images. As can be seen in the table, these values are much greater than 35 dB.

Table 2: PSNR values of the stego images

Images	PSNRs
Airplane	58.8857
Baboon	54.8648
Cameraman	59.0684
Lenna	59.7809
Man	58.6434

Quality of stego

As explained by (Qi *et al.,* 2005), with the shortest route scheme, the expected number of modifications for embedding each message bit, π, is between 0.25 and 0.5. Let π be the expected number of modifications that occurs within a valid block while embedding a single message bit. Therefore, π in this scheme is less than π in the LSB embedding scheme with π = 0.5. So, embedding the message bits creates no obvious visual distortion to the stego image. An example is shown in Fig. 4.

Histogram Analysis

In an image processing context, the histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. For an 8-bit grayscale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values. Fig. 5 shows the histograms of cover and stego images. It is clear that the histograms are almost identical. This is caused by the embedding the message bits in noisy regions of the image. Histogram Analysis as a tool helps in communicating information graphically in a very effective manner. The different types of shapes, sizes and color hold meanings which ultimately help us in the decision making process.

Figure 4: Cover and Stego images

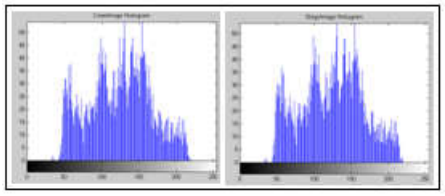

Figure 5: Histograms of cover and stego images

Comparing Capacity

It is clear that the capacity of the proposed method is higher in most images. The mean capacity of the proposed method is about 1206 bits higher than the mean capacity given by the Condith method. Fig. 6 shows the results of computing capacity of proposed algorithm and the Condith method in 829 images.

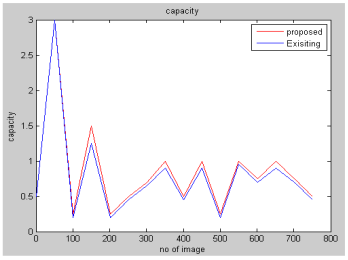

Fig. 6. Embedding capacities of the proposed method (solid) and the Condith method (dashed).

χ2 attack in Spatial Domain

The simplest statistical test for detecting randomness is the χ2 (Chi-Squared) test which sums the square of the discrepancies. Fig. 7 shows the results of the χ2 attack on cover and stego images. Figure show that the χ2-test fails to detect the stegos since the embedding probabilities never remain unity for some percentage of the areas of the image.

ROC Curve Analysis

For comparing the embedding security of proposed method to that of other methods, ROC (Receiver Operating Characteristic) curves are used. We embed our image databases with the minimum value of the maximum capacity of the proposed method and the Condith method. The Fisher linear discriminant classifier was trained with 104 features (Ramezani *et al.,* 2010) derived from 580 cover and corresponding stego images. Statistics of the histogram, wavelet statistics, amplitudes of local extrema from the 1D and 2D adjacency histograms, histogram characteristic function center of mass and co-occurrence matrices were used for the feature extraction process. The generalized eigen vector obtained from training the classifier was used to compute the ROC curve for the remaining 249 cover and corresponding stego images. Fig. 8 plots the ROC curves of proposed method and the Condith method. As observed from Fig. 8. The detection accuracy, shown as the area under the ROC curve, is lower for the proposed algorithm as compared to the other algorithms. The high classification error is due to the small embedded messages. In order to show the results of the ROC clearly, the embedding message size of each image should be increased. So, the image databases are embedded with the maximum capacity obtained by taking T=5. Fig. 9 shows the results of the classification for the latter case.

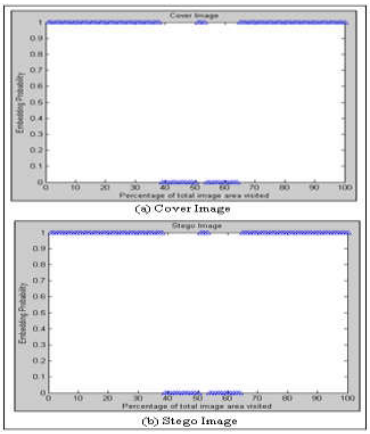

Figure 7. χ2 attack on cover and stego images.

In order to evaluate the detection accuracy quantitatively, 'detection reliability' ρ is used and defined as

$$\rho = 2A\text{-}1 \quad (5)$$

where A is the area under the ROC curve. The accuracy is scaled to obtain ρ = 1 for a perfect detection and ρ = 0 for no detection case. The detection reliability values for the proposed and the reference methods are shown in Table 3.

Table 3: The detection reliability

Method	*ρ(T=5)*	*ρ (T=10)*
Condith	0.1466	0.0802
Proposed method	0.112	0.0789

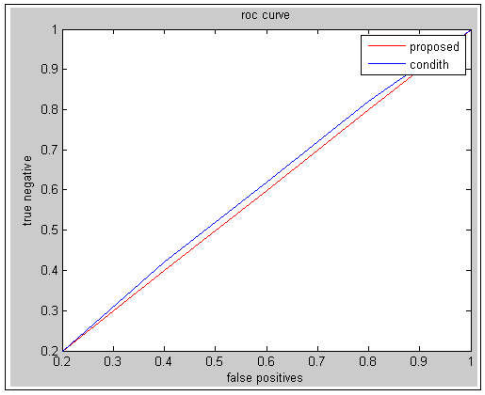

Figure 8. ROC curve
(message size obtained by T=10)

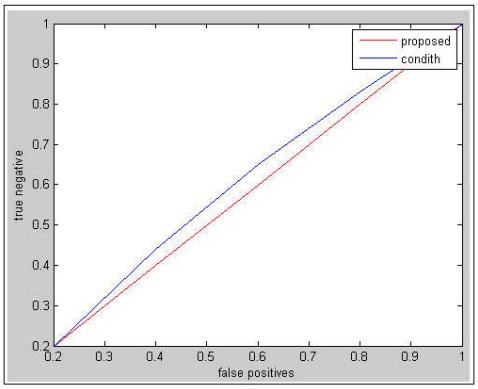

Figure 9. ROC curve
(message size obtained by T=5)

Conclusion

The work dealt with the techniques of a novel steganography model as related to gray scale image. A new and efficient steganographic method with high embedding capacity for embedding the secret message into image without producing any major changes has been shown here. This method also capable of extracting the secret message without the cover image. In this paper we have used the RSA encryption technique and Mod-4 Embedding algorithm to obtain secure stego image. The encrypted form of the message is embedded into the cover image to obtain the stego image. This property enables the method to avoid steganalysis. The existing adaptive steganographic methods have been reviewed and compared to the proposed algorithm. In the senses of the visual imperceptibility, histogram analysis, $\chi 2$ attack, and machine learning based steganalysis, this approach has been verified to be superior to the selected well-known steganography methods.

REFERENCES

Dulce R.H.M., Raul R.C., and F.U.Claudia, 2007. AdaptiveSteganography based on textures in Proceedings of the 17th International Conference on Electronics, Communications and Computers, 34-39.

Franz E., and A. Schneidewind., 2004. Adaptive steganography based on dithering," in Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, Germany,. 56-62.

Huang P., Chang K.C., Chang C.P., and T.M Tu, 2008. A novel image steganography method using tri-way pixel value differencing," Journal of Multimedia, 3.

Hwang, M.S., Lu, E.J.L., and Lin, 2000. A practical (t,n) threshold proxy signature scheme based on the RSA cryptosystem," IEEE Trans. Knowl. Data Eng.,15:1552–1560.

Johnson N.F., and S. Jajodia et al., 1998. Steganography: seeing the unseen," IEEE Computer, 16:26–34.

Lee Y. K., and L. H.Chen, 2000. High capacity image steganographic model," IEE Proc.-Vision, Image and Signal Processing, 147:288–294.

Lin C.F., Wang R.Z., and J.C. Lin, 2001. Image hiding by optimal lsb substitution and genetic algorithm," Pattern Recognition, 34:671–683.

Qi X., and K. Wong, 2005. An Adaptive DCT-Based MOD-4 Steganographic Method," in International Conference on Image Processing (ICIP'05), Genova, Italy,297-300.

Ramezani M., and S. Ghaemmaghami, 2010. Towards Genetic Feature Selection in Image Steganalysis," in 6th IEEE International Workshop on Digital Rights Management, Las Vegas, USA.

Wu D. C. and W.H.Tsai, 2003. A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, 1613–1626.

Wu H. C., N. I. Wu, C. S. Tsai, 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods," in Proc. Inst. Elect. Eng., Vis. Images Signal Process, 611–615.

Yang, C. H., Weng, C. Y, and S. J. Wang *et al.,* 2008. "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, 3(3): 488-497.

****