Contemporary Engineering Sciences, Vol. 8, 2015, no. 12, 525 - 531
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2015.5240

Clustering Based Steganographic Approach for Secure Data Transfer

M. Sownya

School of Computing, SASTRA University, Thanjavur, India

G. Manikandan

School of Computing, SASTRA University, Thanjavur, India

Abstract

Providing security for the message during transmission is a thought-provoking task. To accomplish this goal many cryptographic and steganographic algorithms are being used. Cryptographic algorithms transform the original message into a cipher text before transmission, whereas the basic idea used in Steganography is to hide the existence of the message in a media. This enables the existence of secret data to be known only to the authorized sender and the receiver. In this paper a newfangled method based on clustering and noise addition is proposed to enhance the security of the hidden data. The proposed method consist of two steps. In the first step the pixels of the cover image are grouped into different clusters using k-means clustering algorithm which is followed by the embedding process. In the Second step a random noise is added to each pixel in all the clusters. Experimental results are compared with existing steganography techniques, which shows the proposed algorithm not only achieves same embedding capacity but also enhances the PSNR of the stego image.

Keywords: Data Hiding, Image Steganography, Security, LSB Technique, K-means Clustering

1 Introduction

Steganography is a practice of achieving security by concealing the information within a message, image or file. Image Steganography is the one in which data is hidden within an image. To be more precise cryptography secures the data by trans-

forming it to unreadable format whereas steganography hides the message by embedding it in a media [8]. It may be a text, audio, video or image.

The strength of any steganographic algorithm depends on the starting position from which the embedding process begins. In the existing systems, different starting positions were chosen and embedding was done. In the proposed system, the aim of clustering is to place the similar elements in a group. Clustering is done in such a way that the intra cluster similarity is high. After clustering, a noise value is added to each pixels of all the clusters in order to enhance security.

The remainder of the paper is organised as follows: Section-2 comprises the literature review and the existing system is hashed out in Section-3. Section 4 contains the proposed system and Experimental results are tabulated in Section-5 and a brief conclusion is furnished in section-6.

2 Literature Review

In [1] for content hiding, steganography is carried out along with combination of OPAP and PI technique and pixel value differencing (PVD) for a colour image to raise the security. This has minimised the MSE values.

Data hiding using simple LSB substitution technique and the usage of OPAP to increase the security is proposed [2]. The advantage of this approach is the reduction in computational complexity. The similarity between the original image and stego image are identified based on the observed results.

The data to be embedded is transmuted with arithmetic code method [3]. In [4] a data lossless method based on genetic algorithm is proposed which operates on spatial domain. Here steganography is modelled as a search and optimization problem. PSNR of the stego image is enhanced compared to the other existing methods.

In [5] the data hiding routines are based on image concretion. An embedding algorithm is proposed in which the change in coefficients are decided by the global image statistics [6]. Discovery of distortions in stego image is done using statistical steg analysis. Also, many existing systems have been examined.

In [7], for hiding data, another method has been proposed. An 8*8 image is chosen and DCT is employed, the secret message is embedded in the diagonal pixels and random bits are substituted in place of the text. This is more robust to attacks.

An effective method for embedding a sneaky data in a gray scale image has been purposed. The differences between gray levels and pixel values are used for identifying the embedding pixels. Enhancement of security and efficiency are prime considerations of this approach [9].

In [10], a new steganographic approach with revised LSB substitution and pixel value differences is used in attaining the data embedding capacity and image lineament. Private k-bit modified substitution is proposed for embedding. This method has heightened security and diminished distortions.

3 Existing System

There are many methods available in the literature to implement image steganography. The primary touchstone for designing steganographic algorithm includes the degree of invisibility, raciness against various onslaughts, unperceivability, payload content etc.

All methods in the existing systems have the embedded pixels in the stego image. The hidden message can be retrieved by performing steg-analysis. Our approach aims at hiding the embedded pixels of the stego image, which raises the security.

The new strategy aims at constructing a stego image where the embedded pixels are hidden which provides an efficient as well as a majorly secure version.

4 Proposed System

The proposed system has been developed by combining the K-Means Clustering Algorithm and LSB substitution technique. In this work we are projecting an approach to heighten the security during message transfer between the intended users. The procedure comprises of two phases namely Engrafting and Extraction. The count of clusters formed is known to the sender and the receiver.

In this approach, clustering of pixels is performed based on k-means clustering. The secret message is embedded in the pixels of the first cluster. After embedding the secret data in all the pixels of the first cluster, the process continues with the second cluster and so on. After completing the embedding process a noise value is added to all pixels in each cluster which results in the final stego image which is transmitted.

The steps involved in each phase of this work are summarized as follows.

A. ENGRAFTING PHASE

Step1 : The arcanum message is decided by the sender prior to transmission.
Step2: A cover image is chosen.
Step3: The pixels of the image are clustered using K-Means Clustering algorithm.
Step4: The message is imbedded in the cover image using LSB substitution
Step5: A noise value is added to the pixels of each cluster.
Step6: The resultant Stego image is transmitted to the receiver.

B. EXTRACTION PHASE

Step 1: The stego image is received by the receiver.
Step 2: The stego image is clustered using K-Means Clustering algorithm.
Step 3: The noise value is removed from the transmitted stego image.
Step 4: Message is educed from the pixels of the clusters.
Step 5: The arcanum message is regained.

C. CASE STUDY

For the case study a 5*5 Barbara image is taken from the pool and proposed approach is explained with it. The steps involved are explained and figured below.

Step 1: Pixel region of image for implementation is as shown in the *Fig. 1a*.

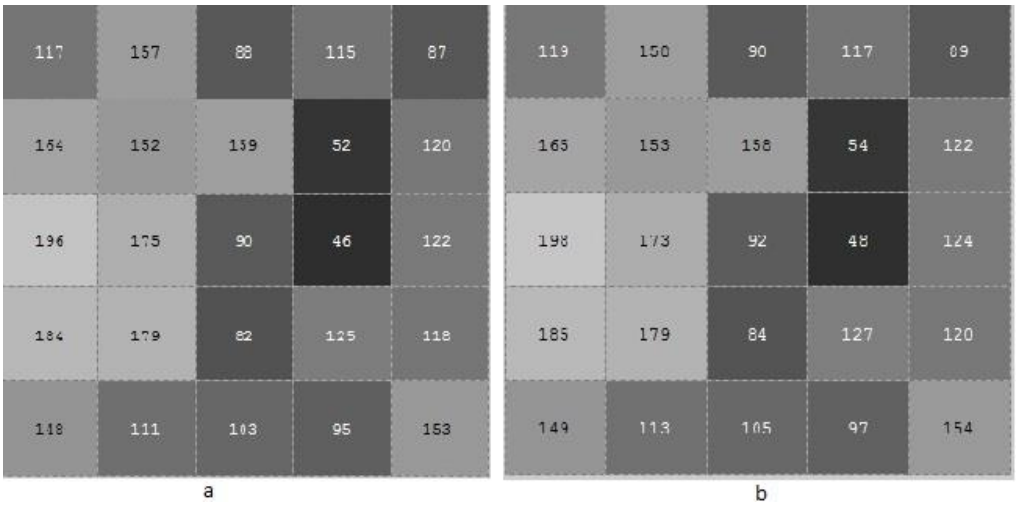

Fig 1. Pixel region a.) Before embedding message, b.)After embedding message

Step 2: The above image is clustered using K-Means Clustering where k=2 as shown in *Fig. 2*

```
>> p1

p1 =

   157   164   152   159   196   175   184   179   148   153

>> p2

p2 =

  Columns 1 through 14

   117    88   115    87    52   120    90    46   122    82   125   118   111   103

  Column 15

    95
```

Fig. 2. Cluster values for image

```
bfr =

   157   164   152   159   196   175   184   179


aftr =

   158   165   153   158   198   173   185   179
```

Fig. 3 Clusters values before and after embedding secret data

Step 3: The message is embedded and noise value is added and corresponding stego image is shown in *Fig. 1 b*. After embedding process and noise value addition, the value changes are shown in *Fig. 3.*

5 Experimental Analysis

The above explained experiments are carried out in MATLAB 8.3 and the snapshots of the input images with its corresponding histograms are represented in *Fig. 4.* The upshot and its gibing histograms are represented in *Fig. 5.*

To appraise the quality of the stego image obtained Mean Squared Error and Peak Signal to Noise Ratio (PSNR) is gauged.

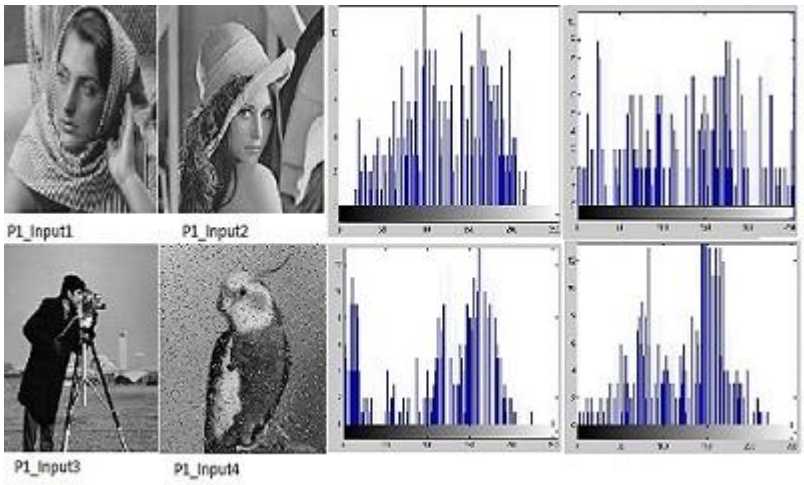

Fig. 4. Input images and corresponding Histograms.

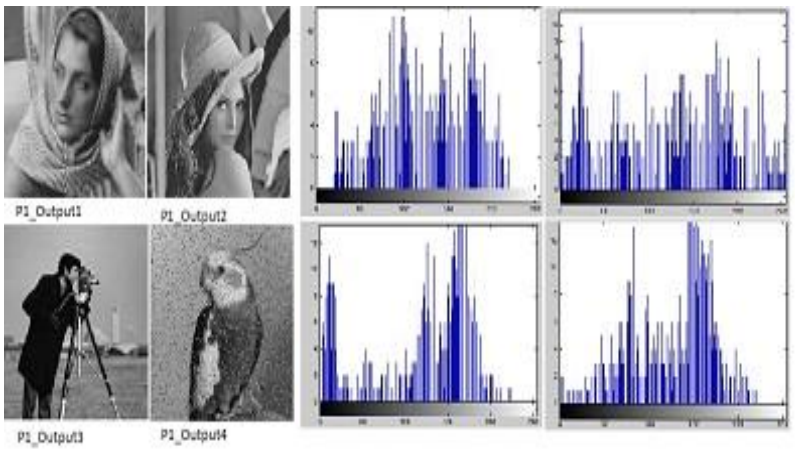

Fig. 5. Stego images and corresponding Histograms

Table I. Variations Observed in Stego Image and Input Image

Input Image	**Stego Image**	**After Embedding**	
		MSE	**PSNR**
Input 1	P1_output 1	0.011	66.31
Input 2	P1_output 2	0.003	72.90
Input 3	P1_output 3	0.003	72.90
Input 4	P1_output 4	0.007	68.05

6 Conclusion

In this paper we have confronted a steganographic approach based on K-Means Clustering and noise addition for secure message interchange. From our experimental outcomes it has been observed that our approach provides a stego image which has an acceptable quality than the stego images obtained by applying existing methods. The result justifies that the potency of the proposed method depend on the number of clusters and the pixels that are picked out for the embedding process. In future this work can be continued with colour images.

References

[1] R. Amirtharajan, Adharsh, D. Vignesh, V. R. John Bosco Balaguru, PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography, International Journal of Computer Applications, 9(2010), 31-37. http://dx.doi.org/10.5120/1275-1801

[2] C. K. Chan, L. M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition, 3(2004), 469–474. http://dx.doi.org/10.1016/j.patcog.2003.08.007

[3] Gomathymeenakshi, M., Sruti, S., Karthikeyan, B., Nayana, M., An efficient arithmetic coding data compression with steganography, IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, ICE-CCN 2013, 6528520, 342-345. http://dx.doi.org/10.1109/ice-ccn.2013.6528520

[4] Hamidreza Rashidy Kanan, Bahram Nazeri, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Expert Systems with Applications , 41(2014), 6123–6130 http://dx.doi.org/10.1016/j.eswa.2014.04.022

[5] Karthikeyan, B., Chakravarthy, J., Ramasubramanian, S., Amalgamation

of scanning paths and modified hill cipher for secure steganography, Australian Journal of Basic and Applied Sciences, 7(2012), 55-61.

[6] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security Privacy Magazine, 3(2003), 32–44. http://dx.doi.org/10.1109/msecp.2003.1203220

[7] Stuti Goel, Arun Rana, Manpreet Kaur, ADCT-based robust methodology for image steganography, International Journal of Image, Graphics and Signal Processing (IJIGSP), 11(2013), 23-34. http://dx.doi.org/10.5815/ijigsp.2013.11.03

[8] William Stallings,Cryptography and Network Security Principles and Practices, Pearson Education, 2006.

[9] Y. D. C. Wu, W. H. Tsai, A steganographic method for images by pixelvalue differencing, Pattern Recognition Letters, 9(2003), 1613–1626. http://dx.doi.org/10.1016/s0167-8655(02)00402-6

[10] Xin Liao, Qiao-yan Wen, Jie Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, Journal of Visual Communication and Image Representation, 22 (2011), 1-8. http://dx.doi.org/10.1016/j.jvcir.2010.08.007

Received: February 25, 2015; Published: May 21, 2015