ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

A New Approach to Securing Images

Vandana M.Ladwani[1], Srikanta Murthy K[2]

Asst.Professor, CSE Department, PESIT(BSC),Bangalore,India[1]

Professor, CSE Department, PESIT(BSC),Bangalore,India[2]

Abstract: Steganography is the art and science of writing hidden messages in such a way that no one apart from sender and intended recipient even realizes that the communication is going on in the first place. It can also be used to authenticate the images. Steganography techniques are categorised into spatial domain and frequency domain techniques. For hiding secret information in images, there exists variety of techniques like LSB, PVD, HoEMD. This paper presents a modulus and cryptography based technique to authenticate the images and can be used to prevent image forgery. The analysis on all the previously implemented techniques and proposed method is done and it has been proved that proposed method has a better PSNR value, hence leading to better image quality.

Keywords: Steganography, spatial, encryption, frequency, DES

I. INTRODUCTION

Social networking has a great impact on society. Information security is very important issue in social networking. Encryption is used to achieve secured message communication. But encryption attracts the eavesdroppers. Steganography is defined as the process of hiding message in images .It can be used for two purposes first being we can secretly transmit the information by hiding messages in image that does not attract attention to itself as an object of scrutiny. Other purpose is, the hidden message can be used to authenticate the images and can be used to prevent image morphing. Key points important in steganography are Embedding capacity and quality of the image after embedding the hidden message.

II. LITERATURE SURVEY

Steganography techniques are mainly classified on the basis of the domains in which we try to embed the data in the image. There are two domains in which various operations can be performed on the image spatial domain and the frequency domain. There are number of techniques using which data can be embedded in the image. Also there exists number of techniques using which hidden data can be retrieved from the image.

In the spatial domain simplest technique used is the LSB substitution.Kurak proposed a technique in which one image can be hidden in another image by replacing the LSB of the cover image by the Most Significant Bit (MSB) of the hidden image[1]. Chi-Kwong Chan, L.M. Cheng proposed data hiding by simple LSB substitution method[4].Human eyes cannot perceive the change in the image achieved by altering the LSB. They applied OPAP (Optimal Pixel Adjustment) after applying simple LSB substitution. The experimental results of their proposed approach proved that stego-image is visually indistinguishable from the original cover-image and the performance of LSB with OPAP is better than both the processes done independently

Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin proposed image hiding by optimal LSB substitution and genetic algorithm[7].Genetic algorithm was proposed to solve the problem of hiding important data in the rightmost *k* LSBs of the host image when k is very large. Experimental results reveal the practicability and superiority of the proposed method.

Frequency domain steganographic methods are based on DCT, DWT, DFT. Chin-Chen Changa, Tung-Shou Chen b, Lou-Zo Chung proposed steganographic method based upon JPEG and quantization table modification [11]. The proposed method modifies the quantization table to improve the quality of stego image without significantly decreasing the hiding capacity. Secret message is hidden in the image by modifying DCT-quantized coefficients of the middle frequency components of the cover image. Finally, a JPEG stego-image is generated. The method was compared with a JPEG hiding-tool Jpeg–Jsteg. It was proved from the experimental results that the proposed method has a larger message capacity than Jpeg–Jsteg. The proposed scheme can withstand visual and statistical attacks.

Chin-Chen Chang, Chia-Chen Lin, Chun-Sen Tseng, Wei-Liang Tai proposed reversible hiding in DCT-based compressed images [13]. This paper presents a lossless and reversible steganography scheme for hiding secret data in each block of quantized discrete cosine transformation (DCT) coefficients of JPEG images. In this scheme, the two successive zero coefficients of the medium-frequency components in each block are used to hide the secret data. Experimental results also confirm that the proposed scheme can provide expected acceptable image quality of stego-images and successfully achieve reversibility

Abdul wahab and Hassan [15] propose a data hiding technique in the DWT domain. Both secret and cover images are decomposed using DWT (1st level). Each of which is divided into disjoint 4x4 blocks. Blocks of the secret image fit into the cover blocks to determine the best match. Afterwards, error blocks are generated and embedded into coefficients of the best matched blocks in the HL of the cover image. Two keys must be communicated; one holds the indices to the matched blocks in the CLL and another for the matched blocks in

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

the CHL of the cover. Note that the extracted payload is not totally identical to the embedded version as the only embedded and extracted bits belong to the secret image approximation while setting all the data in other sub-images to zeros during the reconstruction process.

Kong et al. [17] proposed a content-based image embedding based on segmenting homogenous grayscale areas using a watershed method coupled with Fuzzy C-Means (FCM). For each region Entropy was calculated. If Entropy values exceeded a specific threshold four LSBs of each of the cover's RGB primaries were used otherwise only two LSBs for each were used. The drawback of this method was its sensitivity to intensity changes which would affect severely the extraction of the correct secret bits. Kong et al also reported the use of a logistic map to encrypt the secret bit stream which seems venerable to a Chosen-plaintext attack (CPA).

III. PROPOSED APPROACH

In an attempt to make it tough for an eaves-dropper to detect that message is embedded in the image, the message is not just embedded in the least significant bit of the pixel. To send the message from the sender to the receiver the message is first encrypted using DES encryption algorithm ,then using the proposed embedding algorithm the encrypted message is embedded in the image. On the receiver side the message is retrieved back using the proposed method and decryption algorithm. Image is divided into blocks of two pixel size and critical function is evaluated. Based on the value of the critical function, intensity of any one of the pixel is modified to hide the message information.

A. *Proposed Encoding Method*

1) Select a cover image in which data has to be embedded.

2) Enter the message; the message will be encrypted using DES algorithm

3) The encrypted message is converted in to base 5 and then embedded using the proposed embedding algorithm.

4) The final embedded image is called stego image.

5) The stego image and key is send to the receiver

B.Proposed Embedding Algorithm:

1) Image is divided into blocks of two pixels.

2) Critical function is evaluated with the help of formula
f = ((gray1 *1)+(gray2 *2))%(2*n+1)
where n is the block size

3) d is the data byte array if f=d then the pixel is being discarded for data embedding

4) If f!=d then s is evaluated as
s= (d-f) %(2*n+1)

5) If s<=n

```
        If s==1
                gray1++

If s==2
                gray2++

If s>255then
gray1=254
                continue
   else
        position=2*n+1-s

 If position==1
        gray1--

 Else if position==2
        gray2--
```

C. Proposed Decoding Method

1) Select stego image from which message has to be decoded

2) Decryption happens with the help of same key

3) The decrypted message is converted from base 5 to string

4) The original message is returned.

D. Analysis of Stego Image

1)Mean square error for the image is calculated by comparing the intensity values of stego image with that of the original image.

2) Signal to noise ratio is evaluated for each of the image from the data set

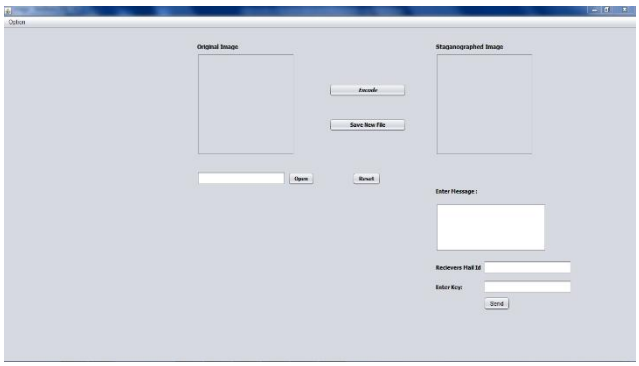
MSE and PSNR value determine the quality of the image containing the hidden message.

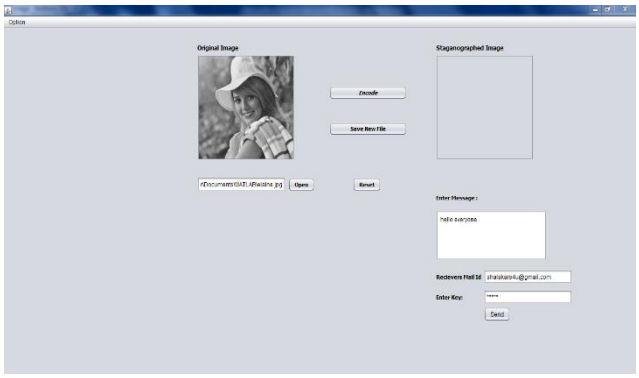
```
for i = 1:size_host;// the size of the original image
      for j= 1:size_host
s = s+(Istego[i,j]-Iold[i,j])^2 ;
end
  where Istego: Pixel intensity of stego image
        Iold: Pixel intensity of original image

  MSE=s/size_host;
  PSNR =10*log10((255)^2/MSE);
```

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

IV. IMPLEMENTATION





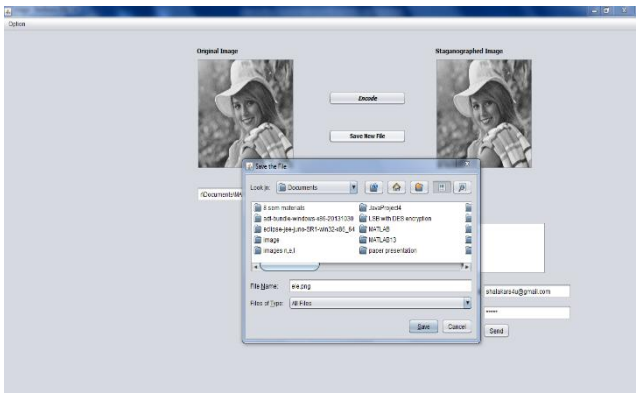
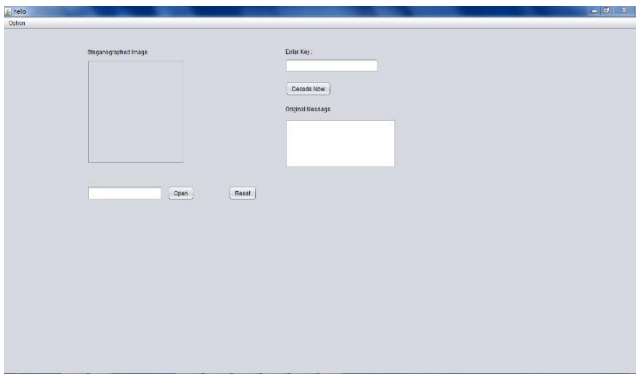
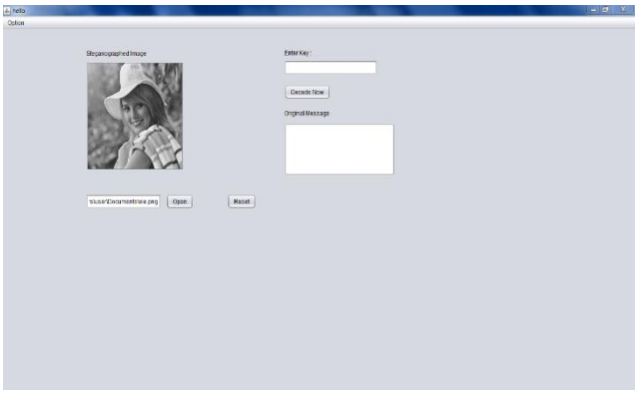


Fig.1. Embedding message in an image





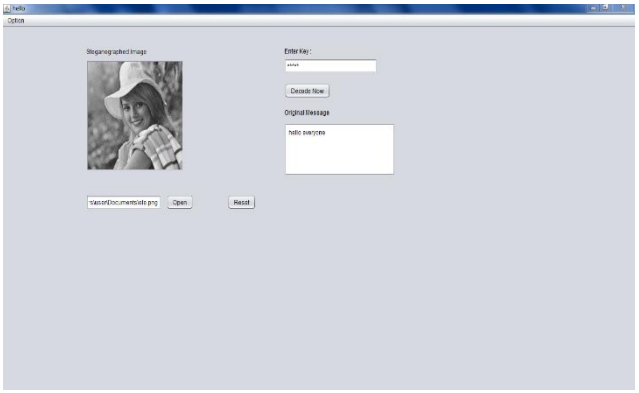


Fig.2. Retrieving message from an image

V. RESULTS

The proposed approach is tested for a dataset of 50 images. Results for few of the images are shown in the table .PSNR and MSE calculation is done using matlab

OTHER APPROACHES				**PROPOSED APPROACH**	
Sr.No.	*Cover Image*	*4 bit LSB PSNR*	*HOEMD PSNR*	*PSNR*	*MSE*
1	Elaine	39.22	31.39	76.69	0.014
2	Lena	39.26	31.22	74.29	0.024
3	Baboon	39.26	31.25	68.84	0.0085
4	Barb	39.26	31.63	66.88	0.0133
5	Zelda	39.25	31.14	67.98	0.0103

VI. CONCLUSION & FUTURE WORK

Based on the statistics it can be inferred that the proposed approach has high PSNR values for all tested images. So the image quality is better. The proposed method can be extended to embed data in video and to prevent malicious editing of the videos and for authentication of the videos.

REFERENCES

[1] Author C. Kurak, J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference, 30 November–4 December, 1992, pp. 153–159

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

[2] H. Kobayashi, Y. Noguchi, H. Kiya, A method of embedding binary data into JPEG bitstreams, IEICE Transactions on Fundamentals J83-D2, 6 (2000) 1469–1476

[3] R. Anderson, F. Petitcolas, On the limits of steganography, IEEE Journal on Selected Areas in Communications 16 (4) (1998) 471–478.

[4] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition 37 (2004) 469 – 474

[5] Chin-Chen Chang, Chih-Yang Lin, Yu-Zheng Wang, New image steganographic methods using run-length approach, Information Sciences 176 (2006) 3393–3408.

[6] V.M. Potdar, S. Han, E. Chang, A survey of digital image water-marking techniques, in: Proceedings of the IEEE Third International Conference on Industrial Informatics (INDIN), Perth, Australia, 10–12 August 2005, pp. 709–716.

[7] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin,"Image hiding by optimal LSB substitution and geneic algorithm", Pattern Recognition 34 (2001) 671}683

[8] A.A. Abdelwahab, L.A. Hassan, A discrete wavelet transform based technique for image data hiding, in: Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, March 18–20, 2008, pp. 1–9

[9] C.C. Lin,W.L. Tai, C.C. Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recogni- tion 41 (12) (2008) 3582–3591.

[10] E.T. Lin, E.J. Delp, A review of data hiding in digital images, in: Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS'99, the Society for Imaging Science and Technology, 1999, pp. 274–278

[11] Chin-Chen Changa, Tung-Shou Chen b, Lou-Zo Chung," "A steganographic method based upon JPEG and quantization table modification", Information Sciences 141 (2002) 123–138

[12] S. Lyu, H. Farid, Steganalysis using higher-order image statistics, IEEE Transactions on Information Forensics and Security 1 (1) (2006) 111–119

[13] Chin-Chen Chang, Chia-Chen Lin, Chun-Sen Tseng, Wei-Liang Tai., "Reversible hiding in DCT-based compressed images", Information Sciences 177 (2007) 2768–2786

[14] M.H. Shirali-Shahreza, M. Shirali-Shahreza, A new approach to Persian/Arabic text steganography, in: Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006), 10–12 July 2006, pp. 310–315.

[15] A.A. Abdelwahab, L.A. Hassan, A discrete wavelet transform based technique for image data hiding, in: Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, March 18–20, 2008, pp. 1–9

[16] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Security and Privacy 1 (3) (2003) 32–44

[17] . J. Kong, H. Jia, X. Li, Z. Qi, A novel content-based information hiding scheme, in: Proceedings of the International Conference on Computer Engineering and Technology, 22–24 January 2009, vol. 1, pp. 436–440

DOI 10.17148/IJARCCE.2015.4149