NOISE SECURES SECRET DATA! BY ACT AS A REFERENCE FOR EMBEDDING

J. Jayaseelan[1] and B. Kruthika[2]
Department of Electronics and Communication Engineering, Parisutham Institute of Technology and Science, India
E-mail: [1]jayaseelan.j89@gmail.com, [2]kruthikabme@gmail.com

Abstract

Data Security is that the most crucial think about a communication network. Data security is achieved by cryptography and data concealing. Steganography is one of the info concealing technique; here any form of signal is concealing by exploitation a picture, audio or video. In an exceedingly spatial domain steganography, most typically the info is embedded into a LSB's of the cover image pixels. As a result of it maintain the standard of the stego image as like as cover image instead of embedded into MSB's. To embedding into a LSB's of cover image (R, G, B plane) researchers are using different types of pixel indicating methods, random embedding, edge based embedding in spatial domain or applying completely different reworks in transform domain. In this paper, for spatial domain steganography noise based embedding technique is proposed; it is entirely different from the out there techniques. In this paper two copies of JPEG, PNG, GIF, or BMP etc., images are used. One is taken as a reference image and noise is added onto that. Supported this reference image knowledge is embedded into the LSB's of cover image. Proposed system using salt and pepper noise for data embedding, it is an ON, OFF noise. Based on added salt, pepper, and no noise portions of reference image completely different range of bits are embedded into the cover image. The result is analyzed by using MSE, PSNR and capacity performance metrics.

Keywords:
LSB, Noise Based Embedding, Pixel Indicator, Salt & Pepper

1. INTRODUCTION

Hiding secret data in any one of carriers such as audio, video, image etc. is called steganography. If the things are visible it is easy to attack. To avoid this evident information hiding technique called steganography introduced [1]. The robustness, capacity of hidden data, computational power shows the power of steganography while compare with other techniques such as cryptography and watermarking. In steganography the term 'cover image' is represented for the carrier in which secret data is embedded. The data which is hided is referred as 'secret data' and the image after embedding the secret data is referred as 'stego image' [1-4]

1.1 STEGANOGRAPHY APPLICATIONS

Steganography has various useful applications such as copyright control; enhancing robustness of image source engines and identity cards, where the individual data's are embedded into their photographs; video, audio synchronization; TV broadcasting. Steganography also used in medical. In medical image system a separation is considered necessary for confidentiality between patient's image data or DNA sequences and their captions; ultimate guarantee of authentication etc [1].

1.2 STEGANOGRAPHY IN SPATIAL DOMAIN

In spatial domain methods secret data is embedded into the LSBs of cover image. One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. In an LSB technique, the binary values of the image are taken for every pixel. Data to be hiding is embedded into these pixels least significant bits. LSB methods typically achieve high capacity and also it maintains the image quality better than the embedding in the MSB's [2, 5].

For example consider, 1st pixel value of cover image is: 10010111. Value of secret data is 0110. From the right, the first four bits are treated as LSB's and last four bits are treated as MSB's. The total decimal value of above pixel is 151. If we embedding this data in LSB then the change becomes 10010110 = 150. But if we embedding in MSB then the value becomes 01100111 = 103. The variation is very large. So LSB embedding is most popular and efficient technique in spatial domain [2, 7, 8].

From the review of researches it was found that, to enhance the standard and capability of the stego image they are using completely different pixel indicator techniques like default pixel indicators, user defined or cyclic indicator for embedding the secret data into the LSB of cover image pixels. To further improve the safety existing approaches uses different substitution, random substitution and low intensity as indicator methods [3]-[9].

2. PROPOSED APPROACH

Information security is the major portion in communication. The techniques used to provide security must be upgrade in a consistent to ensure the quality of imperceptibility. Even the information hiding technique ensures more security with the available techniques; it is an engineer responsibility to provide different methodologies for different requirements. In this paper, A Noise based embedding technique by using Salt & Pepper noise is proposed for steganography which is entirely different from the available techniques.

2.1 CONCEPT

Salt & Pepper is an ON & OFF noise. Salt changes the pixel value into Zero and Pepper changes the pixel value into maximum intensity level. So the added portions of Salt & Pepper noise changes the pixel values of cover image. Based on these changes different number of bits of secret data is embedded into the cover image.

2.2 SYSTEM ARCHITECTURE

Consider a 256 × 256 size image is taken as a cover image. One copy of cover image is taken and Salt & Pepper noise is added into this image. After the addition of noise, the image is referred as 'reference image'. Now the pixel value in the cover image and the reference image are differed based on the added noise. The amount of variation in the pixel value of the reference image can be changed by varying the density of the Salt & Pepper noise. System architecture is shown in Fig.1.

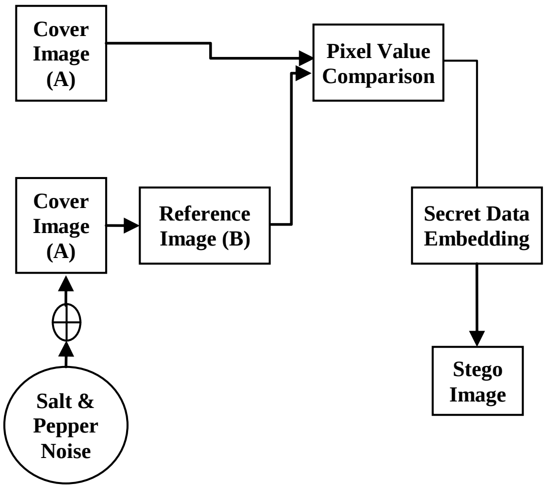

Fig.1. System Architecture of Proposed Approach

For example consider the following 4 × 4 block cover image

Cover Image (*A*)				Reference Image (*B*)			
192	128	136	144	192	0	136	255
220	123	182	214	255	123	0	255
180	140	136	194	180	0	255	194
198	240	220	160	255	240	0	160

In the above example, Salt noise is added with the pixels 2, 7, 10, 15. Similarly Pepper noise is added with pixels 4, 5, 8, 11, 13. The remaining pixels are no noise pixels. The occupation of Salt & Pepper to the particular pixel is varied at every time, because added noise is a random noise.

It can be easily understand that the pixel value is changed in the reference image based on the added Salt & Pepper noise. Now the secret data is embed into the cover image based on this changes. That is secret data is embed into the cover image by the varied pixel positions in the reference image. In this proposed method, three different bits of secret data is embedding as per the values in the reference image.

If the pixel value of reference image and cover image are same then two bits of data is embed into the cover image. If a pixel is added with salt then that value becomes zero and 1 bit of data is embed. Three bits of data is embedding into the cover image for the pepper added pixel values.

For our convenient a cover image of size 256 × 256 is taken, therefore the pixel value of salt added portion is 0 and the pixel value of Pepper added portion is 255.

2.3 SECRET DATA EMBEDDING

Comparative result with reference image and cover image provides the pixel positions of salt, pepper and no noise portions. Now this could be taken as an indicator. Instead of using available existing pixel indicator techniques, this noise indication is expected to provide more imperceptibility. Addition of noise is random, because every time the noise added pixel positions are varying so the clue for steganalysis is very less in this method.

After module 2, the pixel positions of salty, peppery and no noisy positions can be separated. In this module, first the binary value of entire secret data is obtained by using decimal to binary conversion method.

Now 1 bit of secret data is embed into cover image if the pixel position of cover image is added with salt noise. 2 bits of secret data are embed into the cover image, if the pixel is not added with any noise. Finally 3 bits of secret data are embed into the cover image, if the pixel is added with pepper noise. Refer Fig.2.

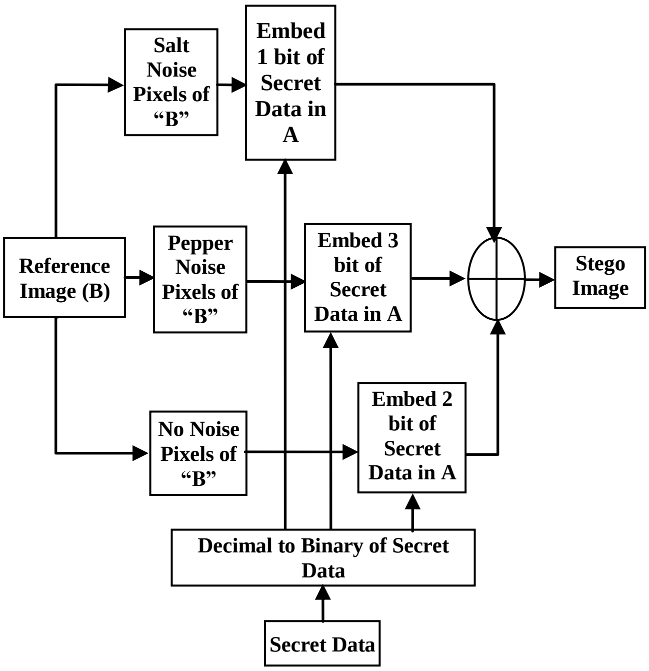
Salt Noise Pixels of "B"
Embed 1 bit of Secret Data in A
Reference Image (B)
Pepper Noise Pixels of "B"
Embed 3 bit of Secret Data in A
Stego Image
No Noise Pixels of "B"
Embed 2 bit of Secret Data in A
Decimal to Binary of Secret Data
Secret Data

Fig.2. Block diagram for secret data embedding

The resultant image after embedding the entire secret data is referred as stego image. This stego image hides the secret data.

3. PERFORMANCE METRICS

3.1 MEAN SQUARE ERROR

MSE measures the average of the squares of the "errors". The average squared difference between an original image and resultant (stego) image is called Mean Squared Error. It dampens small variation between the two pixels but reprimands large ones.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(O_{i,j}-S_{i,j}\right)^2 \qquad (1)$$

where,

M - Number of rows in the image.

N - Number of columns in the image

$S_{i,j}$, $O_{i,j}$ – Pixel intensity of the stego image and cover image.

3.2 PEAK SIGNAL TO NOISE RATIO

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure of quality of reconstruction of lossy compression PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases the reverse may be true. One has to be extremely careful with the range of validity of this metric. It is only conclusively valid when it is used to compare results from the same content.

PSNR is most easily defined via the mean squared error (MSE). It is expressed by,

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^2}{MSE}\right)dB \tag{2}$$

I_{max} - Maximum intensity of the image.

Typical values for the PSNR is 30 to 50 dB, where higher is better.

3.3 BITS PER PIXELS (BPP)

The principal target of this paper is to attain eminent concealing capacity over the single binding image. This engrafting capacity is amended by number of bits engrafted into single pixel. This is assessed as follows,

$$BPP = \left(\frac{C}{P}\right) \tag{3}$$

where,

C = total number of bits engrafted
$P = M \times N$
M = Number of pixels in row of 2D image
N = Number of pixels in column of 2D image

4. IMPLEMENTATION ALGORITHM

Step 1: Read secret data and cover image (*A*) as inputs and find the Corresponding Binary values

Step 2: Take a copy of cover image and add Salt & Pepper Noise with Defined density, Mention this as Reference Image (*B*)

Step 3: Compare the pixel values of cover image and Reference image.

Step 4: If the pixel values of cover image and reference image are equal $A_{ij} = B_{ij}$ then add 2 bits of secret data into the LSBs of cover image pixel A_{ij}.

Step 5: Else if, B_{ij} = 255 then add 3 bits of secret data into the LSBs of Cover image pixel A_{ij}.

Step 6: Else if, B_{ij} = 0 then add 1 bit of secret data into the corresponding LSBs of cover image pixel A_{ij}.

Step 7: Repeat the process until the entire secret data is embedded into the cover image pixels.

Step 8: If the total capacity of cover image pixels is not enough to embed the entire secret data then choose another Cover image.

5. SIMULATION AND EXPERIMENTAL RESULTS

The proposed algorithm is simulated by using Matlab. Imread, uigetfile, imnoise, fopen are the tools used in Matlab. A cover image of size 256 × 256 with 48kb is used to embed the secret data with 9.98kb memory and noise with density 0.2. Corresponding simulation result is shown in the following Matlab figure. This figure includes cover image, reference image and stego image. Embedding the secret data up to Red and Green plane has finished and it is shown in the Fig.3. From the simulation figure it is difficult to identify the difference between the cover image and stego image by the human visual perception

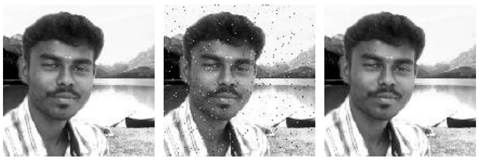

Fig.3. Simulation Result of noise guidance embedding Secret Data

Experimental results for MSE, PSNR and Capacity by embedding the secret data into RED, GREEN & BLUE planes are tabulated below. This tabulation includes the results with the noise density of 0.02, 0.04, 0.06, 0.08 & 0.1.

Table.1. Experimental Results for MSE

Cover Image Density	MSE		
	Red	Green	Blue
0.02	0.2819	0.2403	0.2438
0.04	0.2813	0.2413	0.2444
0.06	0.2806	0.2411	0.2445
0.08	0.2822	0.2405	0.2440
0.1	0.2669	0.2517	0.2483

Table.2. Experimental Results for PSNR

Cover Image Density	PSNR		
	Red	Green	Blue
0.02	53.6302	54.3236	54.2601
0.04	53.6389	54.3058	54.2490
0.06	53.6502	54.3079	54.2486
0.08	53.6245	54.3199	54.2574
0.1	53.8679	54.1224	54.1819

Table.3. Experimental Results for Capacity

Cover Image density	Capacity		
	Red	Green	Blue
0.02	27689	27090	27061
0.04	27649	27103	27091
0.06	27624	27092	27124
0.08	27607	27109	27124
0.1	27282	27279	27279

Table.4. MSE results for various sizes of Images & Secret Data's

Cover Image & Secret Data	Red Plane	Green Plane	Blue Plane
Lena.jpg (15.6kb) & data(17.1kb)	0.2230	0.2003	0.2001
Lena.jpg (15.6kb) & data(133kb)	0.5635	0.5743	0.5698
Peppers.png (133kb) & data(17.1kb)	0.2261	0.2014	0.1975
Peppers.png (133kb) & data(133kb)	0.5251	0.5343	1.0456

Table.5. PSNR results for various sizes of Images & Secret Data's

Cover Image & Secret Data	Red Plane	Green Plane	Blue Plane
Lena.jpg (15.6kb) & data(17.1kb)	54.6474	55.1132	55.1183
Lena.jpg (15.6kb) & data(133kb)	50.6215	50.5392	50.5732
Peppers.png (133kb) & data(17.1kb)	54.5887	55.0905	55.1760
Peppers.png (133kb) & data(133kb)	50.9281	50.8527	47.9371

Table.6: Capacity results for various sizes of Images & Secret Data's

Cover Image & Secret Data	Red Plane	Green Plane	Blue Plane	Total Capacity
Lena.jpg (15.6kb) & data(17.1kb)	46832	46694	46738	140264
Lena.jpg (15.6kb) & data(133kb)	132730	132430	132425	397585
Peppers.png (133kb) & data(17.1kb)	46685	46537	47042	140264
Peppers.png (133kb) & data(133kb)	143719	140474	143370	427563

Experimental Results with various cover image size and secret data size are tabulated in the above Table.4 to Table.6. From the table, it has been observed that our proposed scheme obtains good quality stego image as well as high secret data hiding capacity. It is the major advantage of the proposed scheme.

6. CONCLUSION

In this paper, Information hiding based information security is achieved by using new Noise guidance based Steganography. Salt & Pepper noise is added with a copy of cover image and referred as Reference image. Then the pixel values of cover image and reference image are compared based on the binary values. From the reference image salt, pepper and no noise pixel positions are identified. Based on this identification, 1bit; 2bits; and 3bits of secret data are embedded into the pixel positions of the cover image respectively SALT noise, NO noise and PEPPER noise. Final image with embedded secret data is an output image and it is mentioned as stego image.

From the review of researches it has been identified that the stego image with more than 50dB ensures the imperceptibility. Experimental results prove that our proposed approach provides the healthy stego image with better PSNR and narrowed MSE.

With this achievement this research can be proposed for the ministry of defense. This new technique can also be adapted for various applications based on the requirement.

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", *Journal of signal processing*, Vol. 90, No. 3, pp. 727-752, 2010.

[2] N.F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen", *IEEE Computer*, Vol. 31, No. 2, pp. 26-34, 1998.

[3] J.C. Judge, "Steganography: past, present, future", SANS Institute publication, white paper, 2001.

[4] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography", *IEEE Security and Privacy*, Vol. 1, No. 3, pp. 32-44, 2003.

[5] P. Moulin and R. Koetter, "Data-hiding codes", *Proceedings of the IEEE*, Vol. 93, No. 12, pp. 2083-2126, 2005.

[6] S.B. Sadkhan, "Cryptography: current status and future trends", *Proceedings of IEEE International Conference on Information and Communication Technologies: From Theory to Applications*, pp. 417-418, 2004.

[7] Siwei Lyu and H. Farid, "Steganalysis using higher-order image statistics", *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 1, pp. 111-119, 2006.

[8] David Kahn, "*The code breakers: the comprehensive history of secret communication from ancient times to the Internet*", Scribner, 1996.

[9] J.P. Delahaye, "Information Noyée, information cachée", *Pour la Science*, Vol. 229, pp. 142-146, 1996.