International Journal Of

Recent Scientific Research

ISSN: 0976-3031
Volume: 7(4) April -2016

SECURED DATA TRANSMISSION THROUGH IMAGE ON OPTICAL STEGANOGRAPHY BASED ON NOISE

Thamilvalluvan B., Lakshmi S., Keerthana S.R and Kalaivani K

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

ISSN: 0976-3031

Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 7, Issue, 4, pp. 9888-9891, April, 2016

International Journal of Recent Scientific Research

Research Article

SECURED DATA TRANSMISSION THROUGH IMAGE ON OPTICAL STEGANOGRAPHY BASED ON NOISE

Thamilvalluvan B[1]., Lakshmi S[2]., Keerthana S.R[2] and Kalaivani K [2]

[1,2]Department of Electronics and Communication Engineering Veltech, Avadi, Chennai-600062

ARTICLE INFO

Article History:

Received 15th January, 2015
Received in revised form 21st February, 2016
Accepted 06th March, 2016
Published online 28th April, 2016

Keywords:

Histogram enhanced Image, optical communication, LSB Algorithm, optical steganography.

ABSTRACT

The enhancement of secure data transmission through images on optical communication has been demonstrated experimentally and studied. The tolerance to the dispersion of Optical steganography has been improved. In recent years, the rapid growth of optical communication has become very important to secure information transmission between the sender and receiver. Therefore steganography is introduced, which is used to conceal a secret data in an histogram enhanced image through an optical channel. The dispersion effect is deployed in order to improve the security of the stealth data. In this paper, an algorithm called LSB replacement algorithm is used to conceal a large amount of secret data into the pixels of gray scale image. The dispersion effect due to the larger length of the optical channel used is reduced by increasing the PSNR. The extra dispersion at the transmitter and the receiver functions as a key pair for the optical communication. Eavesdropping is completely eliminated by this method. Finally the performance of this proposal in image through anoptical channel will be evaluated based on the parameters such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR).

INTRODUCTION

Optical steganography based on ASE noise has been experimentally demonstrated to effectively hide a secret data in an input color image (RGB image). The input color image (RGB image) is converted into an gray scale image (range-(0,255)) to increase the speed of transmission rate in optical communication because the data size of input Image is larger than the data size of gray scale image. The data size of input image is given as (256×256×8-R×8-G×8-B) and the data size of gray scale image is (256×256×8) which is much lesser when compared with the data size of the input color image(RGB image) which interns increases the rate of data transmission in optical communication.

An 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The resultant Stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible. The quality of the image, however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality. Histogram equalization plays major role in enhancing the image quality of grey scale image (range-(0,255)). The idea behind enhancement technique is to bring out detail that is obscured, or simply to highlight certain features of an image. A familiar example of enhancement is that we increase the contrast of an image because "it looks better", thus the enhanced image is obtained with the help of histogram equalization.

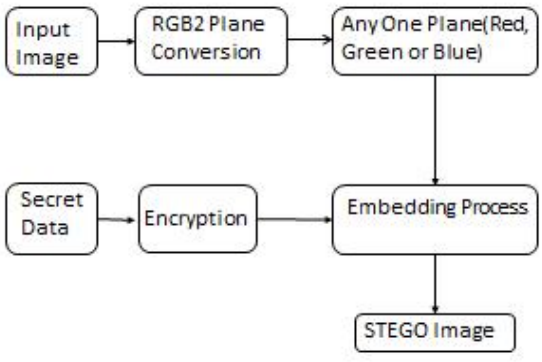

Fig.1 Block Diagram of Embedding Process

Existing System

Hiding data in image using simple LSB Substitution

In this paper, a data hiding scheme by simple LSB substitution is proposed. By applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly

Corresponding author: **Thamilvalluvan B*
Department of Electronics and Communication Engineering Veltech, Avadi, Chennai-600062

improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. Experimental results show that the stego-image is visually indistinguishable from the original cover-image.

Initially the input image (RGB image) is converted into grey scale image as given in fig.2a and then the secret data is embedded into the grey scale image by simple LSB substitution as given in fig.2b.

Fig.2a Color Image converted into Grey Scale Image

Fig.2b Secret Date embedded into the Grey Scale Image by Simple LSB Algorithm

The resulting image with the secret data is called as stego-image in which the quality of the image is very worst with the Simple LSB substitution. Since the quality of the stego-image is very worst, the error rate between the input image and the stego-image is very higher and thus the hidden secret data within the stego-image is easily identified by the eavesdropper which is the drawback in the existing method.

Now the resultant stego-image is traversed within the optical communication channel path along with the optical noise. Then the Simple LSB extraction is applied to extract the secret image hidden within the stego-image. The extracted secret data within the stego-image along the optical communication channel path is visible to human eye because of higher MSE (Mean Square Error) between the input color image and the stego-image.

The main drawback of the existing system is that the higher MSE because of higher error rate between the input image and the stego-image, so if the eavesdropper uses a brute-force approach to search the right LSB substitution, the secret data is easily identified by eavesdropper.

Proposed System

We apply optical steganography method to exchange the secret data between the sender and the target receiver through optical communication channel path.The block diagram of the stealth transmitter and receiver is shown in fig 3a.

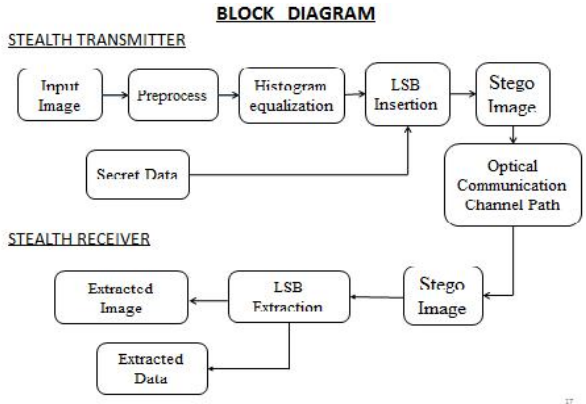

Fig.3a Block Diagram of Stealth Transmitter and Receiver

Preprocessing

Input image is converted into gray scale image by preprocessing. Gray scale images are rendered in black, white, and all the shades of gray in between. The RGB encoding of any gray values is a set of three equal numbers, i.e., (x, x, x), where x is some integer between 0 and 255.For instance, white is (255,255,255), black is (0,0,0) and medium gray is (127,127,127). The higher the numbers, the lighter the gray. The input image is converted into grayscale image using the below equation.

$$x=0.299r+0.587g+0.114b \quad \text{----(1)}$$

Histogram Equalization

The gray scale image is enhanced by histogram equalization method and the resultant image is called Histogram Enhanced Image as in fig.3b.

Fig 3b Histogram Enhanced Image.

Lsb Embedding Algorithm

Now the secret data is embedded into the Histogram Enhanced Image by LSB insertion algorithm. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on.The resultant Stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible. The secret data hidden in the histogram enhanced image is shown in figure 3c.

The quality of the image, however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

Optical Communication Path

When the resultant enhanced image is given into the Optical Communication Channel, ASE Noise (Amplified Spontaneous Emission Noise) which is the optical noise is introduced along with the histogram enhanced image. The wide spectrum and random phase of ASE noise are advantages for hiding the secret data within the histogram enhanced image in which the secret data is hidden and the image quality is very high. The spectral width of ASE noise is around 10nm which is about 1.3THz in terms of frequency.

The secret data is extracted from the resultant image through the optical communication channel path, and then enable the receiver to recover the data precisely by using LSB extraction algorithm.

Lsb Extraction Algorithm

The first bit of message is extracted from the LSB of the first high frequency coefficients and the second some bits of message is extracted from the second reserves coefficients and so on. This process is repeated upto all secret message bits are retrieved and these bits are grouped into 8bits to form a character values. The extraction of desired payload number of bits will be performed by using logical bitwise operators called 'bitand' and 'bitor'.

The main advantage of proposed system is that of enhancing the gray scale image by histogram equalization, which ensures the quality of the image and allows secure transmission of secret data. Also the Mean Square Error (MSE) is reduced by increasing PSNR.

In the proposed system histogram equalization is applied not only to enhance the image quality, it is also used to reduce the error rate. If the quality of the image is enhanced it is clear that the noise in the image is completely eliminated which inturns achieves secure transmission of secrete data hidden in the histogram enhanced image.

EXPERIMENTAL RESULTS

The enhancement of security system for secret data communication through data hiding in images on optical communication is acheived. The dispersion effect is employed in order to improve the secure transmission. The performance of the data transmission through optical steganography was analyzed using the following measures:

- Mean Square Error(MSE)
- Peak Signal to Noise Ratio(PSNR)

Mean Square Error (MSE)

The Quality of the reconstructed image is measured interms of mean square error (MSE).The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\sigma_q^2 = \frac{1}{N} \sum_{j,k} (f[j,k] - g[j,k])^2 \qquad \text{-----(1)}$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image.The impact of MSE is shown in table 1.

Table 1 impact of MSE

	LENA	HORSE
Existing method	0.207672	0.0660706
Proposed method	0.0324	0.00403

Peak Signal to Noise Ratio

The dispersion effect deployed in secure transmission and the mean square error is also reduced by increasing PSNR. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \qquad \text{----(2)}$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes. The impact of PSNR in the proposed system is shown in table 2.

Table 2 impact of PSNR

	LENA	HORSE
Existing method	63.27	68.99
Proposed method	72.54	82.98

Analysis

The tolerance to dispersion to the data rate is described in the optical communication channel path. The dispersion is reduced by increasing the PSNR in terms of data rate.Thus secure transmission is achieved by the decreased error rate. The Dispersion is calculated by using the below equation

$$D(\lambda) = \frac{S0}{4}[\lambda - \lambda_0^4 / \lambda^3] \quad \text{ps/(nm)} \qquad \text{.....(1)}$$

for 1200 nm ≤ λ ≤ 1625nm

Where λ=Operating wavelength.

1. Comparison Between Existing And Proposed Method Analysis On Stego Image Communicating Through Optical Path.

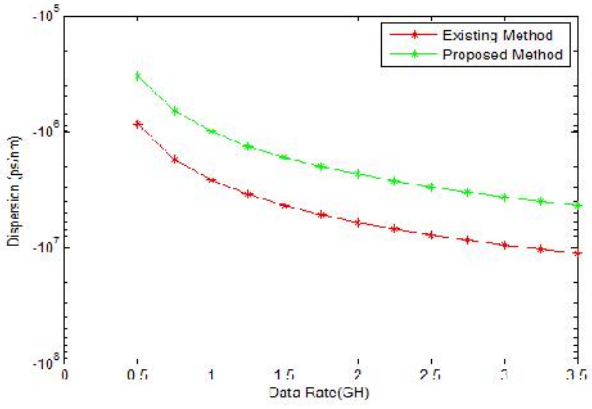

Fig4a Dependence of Dispersion limit on the data rate

2. probability density

The Probability density function of the existing and proposed system is shown in figure 4b.

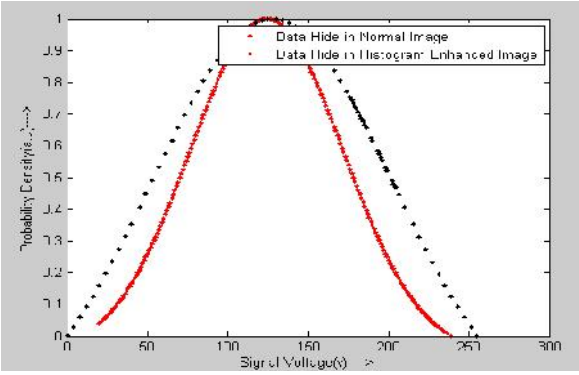

Fig 4b Probability Distribution of Received stealth data

CONCLUSION

The paper explains about the enhancement of secure data transmission through image based on optical steganography and the effect of dispersion on optical steganography based on ASE noise. Deployment of dispersion effect is used to improve the security of the channel. If the data rate is increased, the error rate will decrease and thus the Dispersion effect is compensated .The optical encryption, which encrypts the stealth data as a noisy signal , while optical steganography region hides the stealth data which ensures secure transmission. Thus **EASVESDROPPING** is completely prevented by this method.

References

1. Siti Dhalila mohd satar *et al*., "A new model for hiding text in an image using logical connective" *International journal of multimedia and ubiquitous engineering* vol.10 no.6 pp.195-202, 2015
2. S.A.Khandekar *et al*., "Steganography for text messages using images" vol 4 pp125, 2015
3. Babita Rawat *et al*., "Securing Data in Fiber Optics through Steganography" *International Journal of Advanced Research in Computer science and engineering*. vol 4, issue 6, june 2014
4. B.Wu *et al*., "Optical Steganography based on amplified sponstaneous emission noise," Opt. Exp.vol. 21, no.2, pp.2065-2071, Jan 2013
5. Obaida Mohammed *et al*., "A New Approach For Complex Encrypting And Decrypting Data," *International Journal of computer network and communications* ,vol.5,no.2 March 2013
6. Vikas Tyagi., "Data Hiding in Image using Least Significant Bit with cryptography," *International Journal of Advanced research in computer science and software engineering*,vol.2 issue 4,April 2012
7. B. Wu, Z. Wang, B. J. Shastri, M. P. Chang, N. A. Frost, and P. R. Prucnal, "Temporal phase mask encrypted optical steganography carried by amplified spontaneous emission noise," *Opt. Exp.*, vol. 22, no. 1, pp. 954–961, Jan. 2014.
8. E. Desurvire, "Chapter 5 gain, saturation and noisse characteristics of erbium-doped fiber amplifiers," in *Erbium-Doped Fiber Amplifiers, Principles and Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 2002, pp. 355–357.
9. E. Desurvire, "Analysis of noise figure spectral distribution in erbium doped fiber amplifiers pumped near 980 and 1480 nm," *Appl. Opt.*, vol. 29, no. 21, pp. 3118–3125, Jul. 1990.
10. B. Wu, Z. Wang, B. J. Shastri, Y. Tian, and P. R. Prucnal, "Two dimensional encrypted optical steganography based on amplified spontaneous emission noise," in *Proc. CLEO*, Jun. 2013, pp. 1–2, paper AF1H.5.
11. M. A. Islam and M. S. Alam, "Design optimization of equiangular spiral photonic crystal fiber for large negative flat dispersion and high birefringence," *J. Lightw. Technol.*, vol. 30, no. 22, pp. 3545–3551, Nov. 15, 2012.

****

How to cite this article:

Thamilvalluvan B *et al*.2016, Secured Data Transmission Through Image on Optical Steganography Based on Noise. *Int J Recent Sci Res.* 7(4), pp. 9888-9891.

TSSN 0976-3031