ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 5, Issue - 2, March – April - 2019, Page No. 01 - 07

Secure Data Communication using Information Hiding Algorithm and its Implementation in Visual Cryptography

Manish Choubisa, Department of Computer Science & Engineering , Arya Institute of Engineering & Technology, Jaipur, India

Manish Dubey, Department of Computer Science & Engineering , Arya Institute of Engineering & Technology, Jaipur, India

Abstract

The Visual cryptography scheme is a method to split a secret image into two shares. In this paper, we present a method of Least Significant Bits (LSB) information hiding for Secure Data Splitting Algorithm and Data Embedding Algorithm and based on this, quality will be managed by PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error) control monochromic images. We propose and implement a new steganography technique for images by modifying existing algorithms. This technique uses LSB steganography as our basis and disperses a secret message over the entire image taken by us to ensure that the secret message cannot be get from the image. When we compare with other existing algorithms, we can easily prove that the difficulty of decoding the proposed algorithm is high. The system developed for hiding and extracting files based on the method has a wide range of adaptivity and good applicability.

Keywords: Information hiding, LSB, MSE, PSNR

Introduction

With the rapid development and wide use of Internet, information transmission faces a big challenge of security. People need a safe and secured way to transmit information. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other[1]. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. This technique used to encrypt a image into shares such that stacking a sufficient number of shares reveals the secret images. In visual cryptography there are different technique like sub pixel, error diffusion, Boolean operation etc.

Visual Cryptography provides information security using simple algorithm. This technique allows visual information to be encrypted using some cryptographic schemes and their decryption can be performed by the human visual systems without any complex cryptographic algorithms[2][3]. It encrypts the secret image into shares and the stacking of sufficient number of shares reveals the original image. Shares are usually represented in transparencies.

In this paper, based on C, we use an improved LSB algorithm to replace the least significant bits of the pixels in the cover-up RGB image and validate the algorithm by modeling.

Image information hiding

Generally, the information hiding includes both information embedding algorithms and information extraction algorithms. Embedding is an information hiding process, while extraction is the restoration process of secret information. Therefore extraction operation is the inverse operation of embedding operation.

Typical information hiding algorithm can be divided into the temporal-spatial domain hiding algorithm and transformation domain algorithm according to the different cover-up spaces.

Temporal-spatial domain hiding algorithm

Temporal-spatial domain hiding algorithm uses the method of directly changing the elements of an image

Generally, the contents are hidden in the brightness or color of the image elements. The advantage of the temporal-spatial domain algorithm is that only a very small and inconspicuous change can hide a large amount of secret information. So calculation time can be faster and complexity can be lower. LSB is a kind of hiding algorithm based on temporal-spatial domain.

Transformation domain hiding algorithm

Transformation domain hiding algorithm is to use mathematical transformation to represent the image by using transformed domain such as frequency domain. The information to be hidden is added to the transformed domain coefficients of the cover-up image. The resulting image is generated by inverse transformation. Common transformation domain algorithms include DCT (Discrete Cosine Transform)-based transformation domain algorithms and DWT (Discrete Wavelet Transform)-based the transformation domain algorithms[5].

Traditional LSB method based on temporal-spatial domain

In the theory of LSB Information hiding algorithm watermark information is represented (hidden) by modifying the colour or colour component bit-plane, and adjusting the perceptively unimportant pixels in digital image. The algorithm is to input a secret key into a pseudo sequence generator to create random signals, and then use some rules to create a 2D watermark, which is inserted into the least bits of an image one after another. The watermark is invisible because the information is hidden into the least bits of the image. This way, embedding and hiding of the information is realized.

A computer graphic image is a matrix (block) that is made of values representing each pixel brightness or color level. Let a grey image be made of n*n pixels, the brightness (color level) of each pixel is represented by a binary number of 8 bits, there are 256 grey (color) levels and n*n equal-sized squares, each corresponding to one pixel. Let us use i and j to denote the ith component (pixel or square) of the image (the whole matrix or block) in horizontal direction and the jth component (pixel or square) in vertical direction respectively, then a pixel (square) can be represented by Sij.

The LSB algorithm converts the confidential data into a binary data stream, and then hides the stream into the proper lower bit planes of the image (diagram). The values of part of pixels of the image on the bottom bit plane or several above planes will be replaced by the data to be concealed. since the human eyes are insensitive to certain range of brightness, the changes in LSB have less impact on the cover-up image (information carrier).

Proposed LSB algorithm

Secure Data Splitting Algorithm

The algorithm which is used to split the secure Data into two different shares is given below:

INPUT: Secret Data

OUTPUT: Two different secret shares of input data

Step1: Start

Step2: Clearing variables, closing figures and Clear output screen.

Step3: Read input secret data or color secret image in 256 × 256 standard. If image is not in this standard then convert it into 256 × 256 standard and also conversion RGB into Binary image.

Step4: Initializing the two different shares with pixel values zeros and the width of each share is twice than the width of secret data.

Step5: Finding all the white pixels indexes i.e. pixel values ones, in the secret data and for every white pixel value we store the required values in each of the share.

Step6: Finding all the black pixels indexes i.e. pixel value zeros, in the secret data and for every black pixel value we store the required values in each of the share.

Step7: Overlap these two shares to check the visual cryptography.

Step8: Stop

Data Embedding Algorithm

The steps involved in the Data Shares Embedding algorithm using Least Significant Bit based technique are given below.

INPUT: Two different Shares (Share1 and Share2) from Algorithm 4.1 and two cover images (Image1 and image2)

OUTPUT: Two Stego Image)

Step1: Start

Step2:Read two shares and two cover images. Convert color image into gray

Step3: Check that the shares are not too large for images.

if (maximum length of share> maximum length of image)

Error (shares cannot be embedded in the given images bigger images are required') and exit

end if

Step4: Embedding share1 into the last three LSB's of the image1 intensity

Set k=1

for i=1:height of image1

for j=1:weight of image1

if k <= size of share1

sum=0;

```
            sum=sum+4*share1_vector(k);
                        k=k+1;
           if k<= size of share1
          sum=sum+2*share1_vector(k);
                        k=k+1;
end
if k<= size of share1
       sum=sum+1*share1_vector(k);
k=k+1;
end
if image1(i,j)+sum < 255
embed_image1(i,j)=image1(i,j)+sum;
else
image1(i,j)=image1(i,j)-sum;
 end
else
    i=height of image1;
   j=weight of image1;
end
end
end
```

Step5: Repeat Step4 for embedding share2 into the last three LSB's of the image2 intensity.

Step6. Computing the difference between original image and embedded image

Step7: Calculating the PSNR of these Embedded Images.

Step8: Stop.

Implementation

Information embedding and extracting flow charts are shown as in Fig. 1 and Fig. 2 respectively:

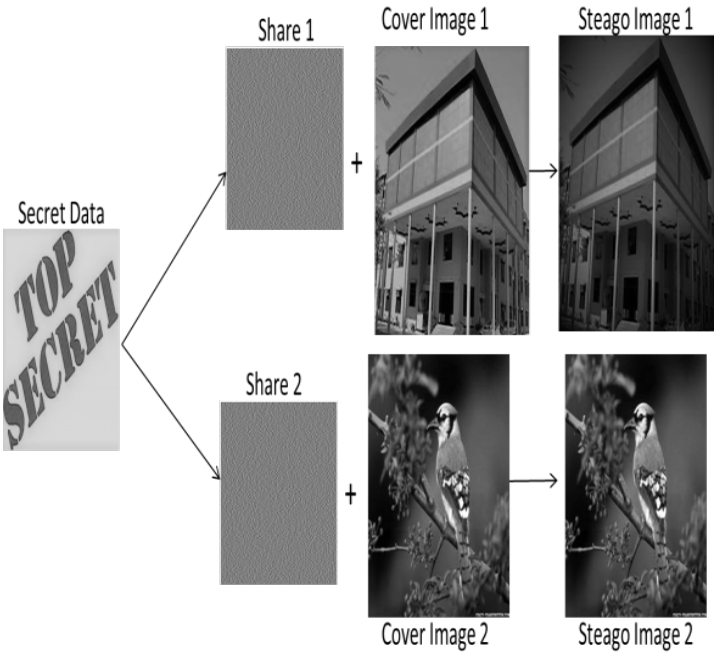

Figure 1. Secret Data Embedding Process using Visual Crptography

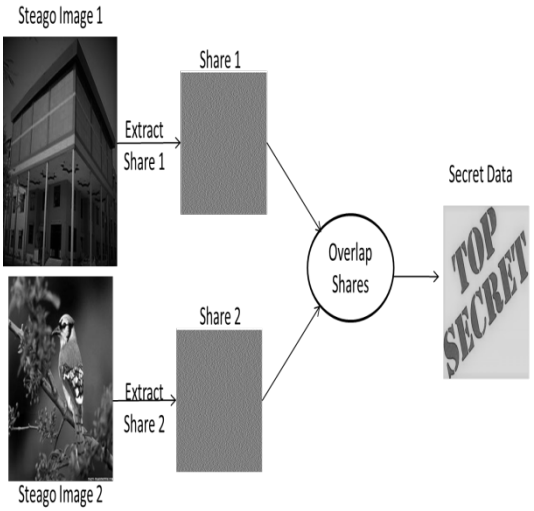

Figure 2. Secret Data Extracting Process using Visual Crptography

Experimental results

Computing Peak Single to Noise Ratio (PSNR)

When PSNR is higher than 30, recomposed image has a very good quality and the eye could hardly tell the difference between the original and the recomposed image.

The smaller the PSNR value is, the larger the difference between images will be. The larger PSNR value implies the better image restoration. Usually, when the PSNR value is above 28dB, the image will have good quality of recovery. For

the given algorithm, the PSNR value of the original image and the recovered image is 28.7595, which shows that the algorithm proposed in this is effective.

The Peak Single to Noise Ratio (PSNR) is a common measure of the quality of Embedded Image.

Calculating PSNR using following formula:

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

The mean square error (MSE) of two images of N x N pixels is defined as:

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(p_{ij} - p'_{ij}\right)^2$$

Where P_{ij} is the original cover image value and p'_{ij} is the embedded image pixel value. The higher the pixel value the better the quality of the reconstructed image[10].

Table 1 shows the PSNR of these three stego images

Table 1: Sample of Images and their PSNR

Image	Resolution	Embedded Share	PSNR (db)
Building	256 × 256	Share one	38.14
Bird	256 × 256	Share two	32.28

Conclusion

In this paper, an implement robust LSB information hiding algorithm is proposed according to human visual theory, a detailed description is given of how to implement this algorithm, and a system is constructed based on this algorithm for image hiding and extraction. The result shows that this new algorithm has many outstanding advantages in the environmental configuration requirement, the time-consuming in running, ease of use and so on. The information hiding and extraction system implemented on MAT Lab platform takes less running time and recourses and is easy to use etc.

The realization of the improved LSB algorithm based on visual cryptography has many advantages: faster calculation and bigger amount of embeddable information than traditional LSB algorithm does. However, the issues of robustness and security still need to be further studied.

On the basis of this, we can make following improvements for the LSB algorithm. For example, we could expand the m sequence into 2D and then use corresponding function to improve the detection process; thereby the robustness can be greatly enhanced. In addition, we could integrate the LSB algorithm with some encryption algorithm to improve its security.

References

1. Jitao Jiang, Xueqiu Zhou, and Xiaohong Liu. “An improved algorithm based on LSB in digital image hidden”, Journal of Shandong University of Technology (Science and Technology), vol. 20(3), 2006, pp. 66-68, doi: cnki:ISSN:1672-6197.0.2006-03-018.

2. Juan Zhou, Shijie Jia, “Design and Implementation of Image Hiding System Based on LSB”, Computer Technology and Development, vol. 17 (05), 2007, pp. 114-116, doi: cnki:ISSN:1673-629X.0.2007-05-034.
3. Jianwei Zhang, Xinxin Fang, Junhong Yan, “Implement Of Digital Image Watermarking LSB”, Control & Automation, vol. 22(10), 2006, pp. 228-229, doi: cnki:ISSN:1008-0570.0.2006-10-083.
4. Qian-lan Deng Jia-jun Lin, “A Steganalysis of LSB based on Statistics”, Modern Computer, No.1, 2006, pp. 46-48, doi: cnki:ISSN:1007-1423.0.2006-01-010.
5. Jian-quan Xie, Chun-hua Yang. “Adaptive hiding method of large capacity information”, Journal of computer applications, vol. 27(5), 2007, pp.1035-1037, doi: CNKI:ISSN:1001-9081.0.2007-05-001.
6. Hongwei Lu, Baoping Wan, “Information Hiding Algorithm Using BMP Image”, Journal of Wuhan University of Technology, vol.28(6), 2006, pp. 96-98, doi: cnki:ISSN:1671-4431.0.2006-06-027.
7. P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Young , (2008) “A New Copyright Protection Scheme with Visual Cryptography”, Second International Conference on Future Generation Communication and Networking Symposia. pp. 60-63.
8. Y. Wei-Qi, J. Duo,M. S. Kankanhalli, (2004) “Visual Cryptography for Print and Scan Applications”. International Symposium on Circuits and Systems. pp- 572-575.
9. S. Gravano,(2001) Introduction to Error Control Codes, Oxford University Press, USA.
10. D. C. Wu and W. H. Tsai, “Spatial-domain image hiding using image differencing,” TRANSFORMING LSB SUBSTITUTION FOR IMAGE-BASED STEGANOGRAPHY 1211 IEEE Proceedings of Vision, Image and Signal Processing, Vol. 147, 2000, pp. 29-37.