Encryption of an Image Using Least Significant Bit Substitution Method and Arnold Transformation

Girish Khandappalavar , Shrividya G
Department of Digital Electronics and Communication,
NMAMIT, Nitte

Abstract: Image steganography is becoming an important area in the field of steganography. As the demand of security and privacy increases, need of hiding their secret information is also increasing. If a user wants to send their secret information to other persons securely, he can send it by using image steganography. In this paper, a new efficient image encryption technique is presented. It is based on a combination between least significant bit (LSB) and Arnold's cat map algorithms. The algorithm aims at achieving a better security than the existing ones.

Keywords: Least significant bit (LSB), Arnold's cat map, image hiding.

1. INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place. It is accomplished by hiding information in other information. It is an art of concealing a message in a cover without leaving a remarkable track on the original message. The goal of Steganography is to mask the very presence of communication making the true message not discernible to the observer. There are 4 different types of steganography

1. Text 2. Image 3. Audio and 4. Video

Steganography is a process of hiding the secret data into a cover object to protect it from unauthorized access. It is a technique of invisible communication which hides the existence of the message. If the cover object used is an image, the steganography is known as image steganography. It has many applications like online transactions, military communication etc.
Image hiding techniques embed a secret image into another image. The fusion of the secret image and the cover image is the resultant stego-image. Using the image hiding techniques, existence of the secret image in the final image will be invisible by an unintended observer, so that it can be relocated carefully [1].

In the basic steganographic process, the secret message is hidden into a cover object. The cover object can be any either a text, an image, an audio file or a video clip. A secret key is also used and the secret message is embedded into the cover object using the secret key. This new message obtained is called stego message. The stego message is transmitted over the public channel. The receiver gets the message and retrieves the message using the stego key which is same as used by the sender. In this way security is achieved by hiding the existence of the message.

The rest of the paper is organized as follows: section 2 gives an insight into the proposed work. Section 3 details the implementation of an image hiding technique. Section 4 presents the implementation of an Arnold cat map transformation. Results and analysis are presented in Section 5. Finally section 6 gives the concluding remarks.

2. PROPOSED WORK

In this paper, a new efficient image encryption technique based on a combination between least significant bit and Arnold's cat map is presented. Figure.1 shows the block diagram of the proposed image encryption technique [2].

The proposed encryption technique follows these steps:-

1. Apply hiding technique to the original image. It is found that the encrypted image histogram is the same as the original image histogram. That is the reason for adding the hiding technique.
2. Apply the Arnold cat map transformation to the whole image.

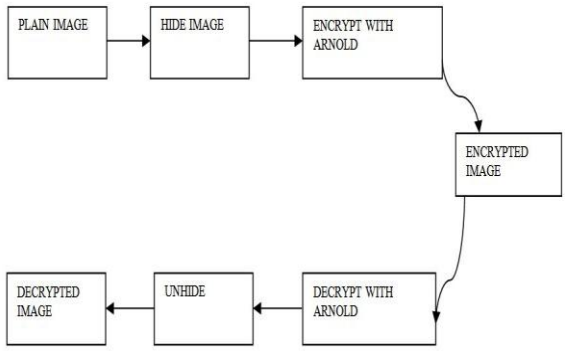


Fig.1: Proposed Image Encryption Technique

3. IMPLEMENTATION OF IMAGE HIDING

Every pixel in an image indicates a color and the each image is made up of pixels. The lower values of the pixel in a gray - scale image signifies dark areas and the higher values signify light areas. So in order to adjust the shades of the image its values can be adjusted and 8 bits are required to represent these values.

For example, consider the following 8-bit binary sequence: 10110011. Summing up all these values where 1 exists, will yield a result of 179. The right-most value is the LSB of this sequence. This value essentially determines whether the total sum is odd or even. If the LSB is a 1, then the total will be an odd number, and if 0, it will be an even number. However, changing the LSB value from a 0 to a 1 does not have a huge impact on the final result [3].

Each 8-bit binary sequence is used for expressing the color of a pixel for an image, so changing the LSB value from a 0 to 1 does not impose a major change and it is unlikely to be noticed by an observer. In fact, the LSBs of each pixel value could be potentially modified, and the changes would still not be visible. This provides an enormous amount of redundancy in the image data, which means that we can effectively substitute the LSBs of the image data, with each bit of the message data until the entire message has been embedded.

The block diagram of the image hiding is as shown below figure 2.

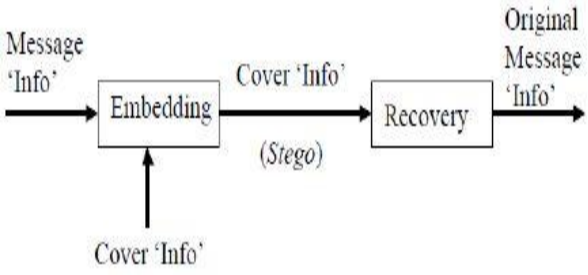


Fig.2: Basic Block Diagram of Image Hiding

The steps used in the LSB method are:-

I. To hide

1. Get the input cover image and message image.
2. Resize the message image to be same as that of the cover image.
3. Shift the message image pixel values over four bits to right.
4. Make last four bits (LSBs) in the pixel values of the cover image to zero.
5. Finally add the images obtained from step 3 and 4 to get final image.

II. To unhide

In order to recover the secret image at the receiver's side the pixel of the image that is shifted left at the LSB process should be shifted right.

1. Get the retrieved image as input.
2. Shift the message image pixel values over four bits to the left.
3. Message image is obtained.

4. IMPLEMENTATION OF ARNOLD TRANSFORMATION

Arnold's cat map (ACM) in recognition of Russian mathematician Vladimir I. Arnold, who discovered it using an image of a cat. It is a simple and elegant demonstration and illustration of some of the principles of chaos – namely, underlying order to an apparently random evolution of a system. An image (not necessarily a cat) is hit with a transformation that apparently randomizes the original organization of its pixels as shown in figure 3 [2].

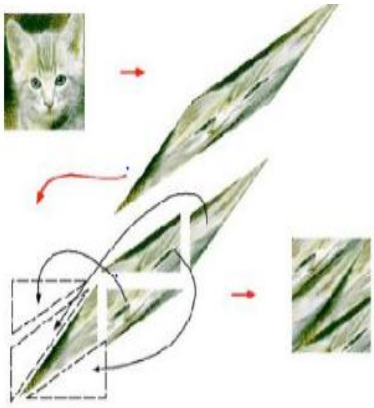


Fig.3: Arnold Cat Map Transformation

The pixels rapidly degenerate into a television-static of chaos by iteration number five, with some unintelligible order prominent in a number of iterations prior to the original image reappearing on the fifteenth iteration. Therefore, the image is said to have a period of fifteen. The ACM has one main disadvantage: after a number of iterations of the ACM, the original image will return, and the histogram of the encrypted image is the same as the histogram of the original image. This is due to the fact that the pixel values themselves didn't change.

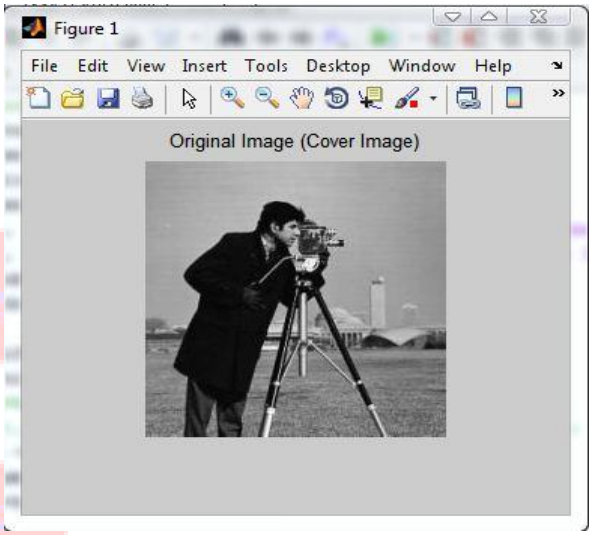
When Arnold transform applied to a digital image randomizes the original organization of its pixels and the image become imperceptible or noisy. Arnold transform is a simple but powerful transform and digital image encryption can be achieved by using this transform. Arnold Transform is commonly known as cat face transform and is only suitable for N×N images digital images. It is defined as [4]

$$\begin{matrix} x' \\ y' \end{matrix} = \begin{matrix} 1 & 1 \\ 1 & 2 \end{matrix} \begin{matrix} x \\ y \end{matrix} \pmod n$$

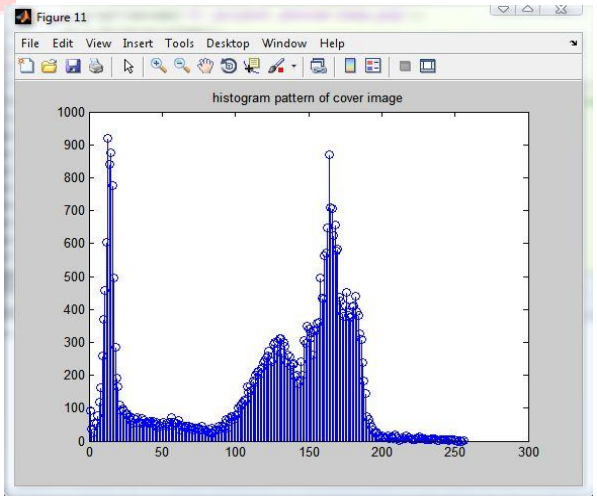
Where (x , y) are the coordinates of original image, and (x′, y′) are the coordinates of image pixels of the transformed image. Transform changes the position of pixels and if done several times, scrambled image is obtained. N is the height or width of the square image to be processed. Arnold Transform is periodic in nature. The decryption of image depends on transformation periods. Period changes in accordance with size of image. Iteration number is used as the encryption key. When Arnold Transformation is applied, the image can do iteration, iteration number is used as a secret key for extracting the secret image.

5. RESULT AND ANALYSIS

The hiding of an image is implemented under matlab 7.6. An image "cameraman.jpeg" is taken as a cover image to hide a secret image as shown in figure 4(a) and its histogram pattern as shown in figure 4(b). Then "lena.jpeg" is taken as a secret image and its histogram pattern as shown in figure 5(a) & 5(b). The encrypted stego image and its histogram pattern are shown in figure 6(a) & 6(b).

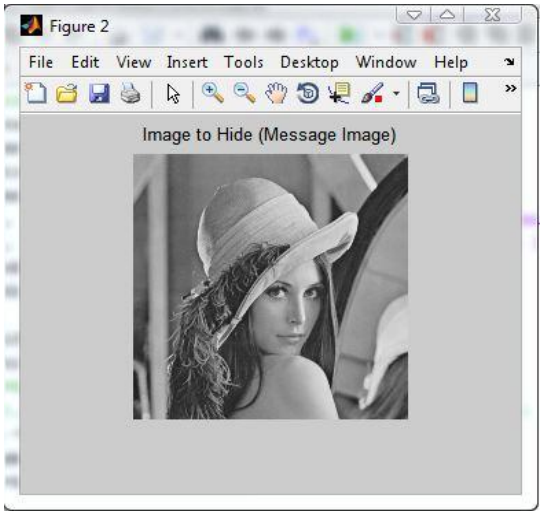


(a)

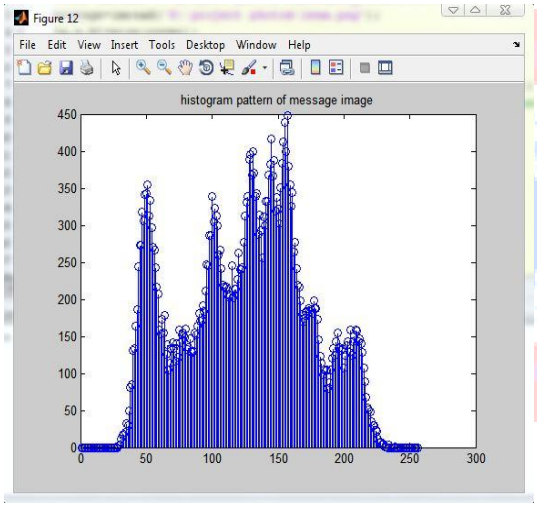


(b)

Fig.4: Cover Image and its Histogram Pattern

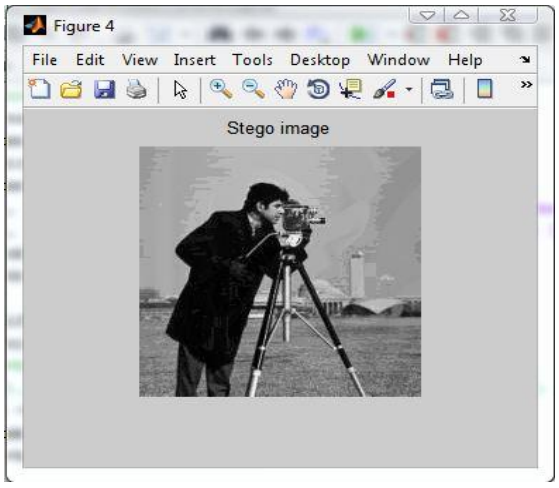


(a)

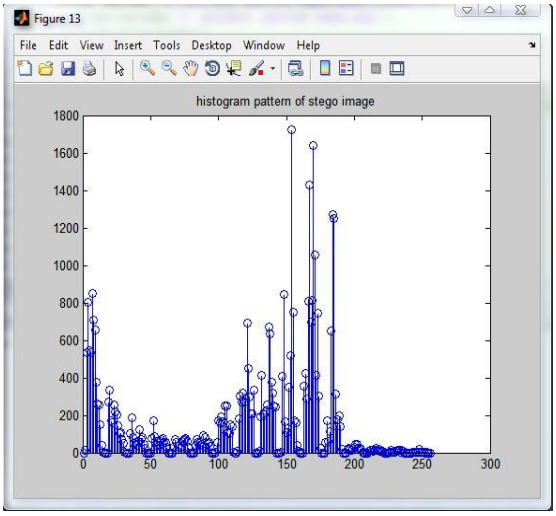


(b)

Fig. 5: Secret Image and its Histogram Pattern

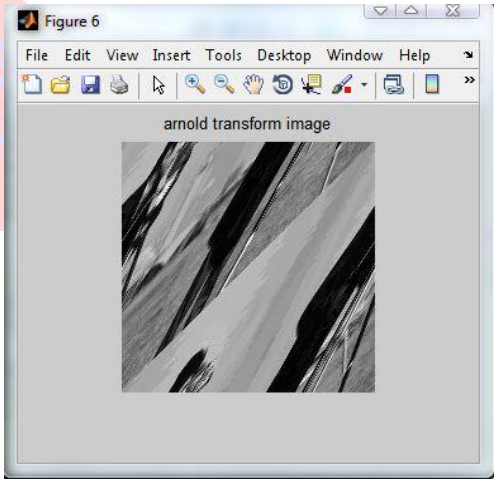


(a)

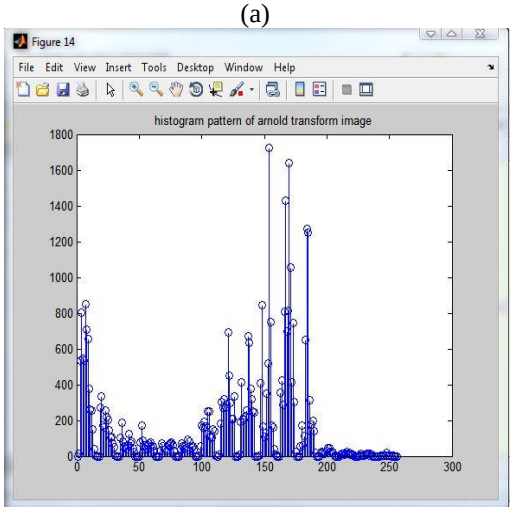


(b)

Fig. 6: Stego Image and its Histogram Pattern



(a)



(b)

Fig. 7: Arnold Transformed Image & Histogram Pattern

After hiding one image on another image, stego image is obtained. By using the stego image, Arnold transformation algorithm is applied to perform image scrambling. The figure 7(a) & 7(b) shows Arnold transformed image and its histogram pattern.

6. CONCLUSION

In this work, a new encryption technique based on a combination between Arnold's cat map and image hiding technique is introduced. LSB based techniques pose a difficult challenge to a stego-analyst as it is difficult to differentiate final image and the cover image which is given as input. The differences between them will be very slight. Again by using image scrambling to encrypt the image to improve the security of image. It can more effectively improve the security of image, lead decipher even more difficult.

7.REFERENCES

[1] Mr. Vikas Tyagi; "Data Hiding in Image using least significant bit with cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 ISSN: 2277 128X.

[2] Amr M. Raid; Amr H. Hussein; Atef Abou EL-Azm; "A New Selective Image Encryption Approach using Hybrid Chaos and Block Cipher" The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May.

[3] R. Rathna Krupa; " An Overview of Image Hiding Techniques in Image Processing" The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 2, No. 2, March-April 2014.

[4] Y. Wang; T. Li; "Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System," Intelligent System Design and Engineering Application (ISDEA), 2010 International Conference on , vo1.2, pp.449-451, 13-14 Oct. 2010.

[5]Himanshu Gupta; Prof. Ritesh Kumar; Dr. Soni Changlani; "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method" ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June 2013.