Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 4, April -2015

A Steganography Approach over Color Images based on Image Edge

Nanera Vimal D.[1], Mr. Mohammed Sayeemuddin Shaikh [2]

[1]Student, Electronics and Communication Department, LJIET, Ahmedabad
[2]Assi. Prof., Electronics and Communication Department, LJIET, Ahmedabad

Abstract — *As communication systems are evolving at fast pace, the security is main concern. Cryptography is the method that can be used for the security purpose when the data transmission is required. Though cryptography is used, third party can hack the information that is transmitted. Steganography is the method that is used to hide the information behind a carrier information, so that the third party cannot even detect that the information is hidden. The digital images are the popular carriers because of their frequency on the Internet. We propose a kind of steganographic algorithm based on the image edge processing in this paper. Firstly, the mathematical morphology is applied on the cover image. The secret message is first encoded and then converted into binary bits. Then, the encoded message is successfully embedded into cover image using F5 Algorithm. Results shown in this paper demonstrates the advantages like the small changes in image quality, strong ability in anti-attack and the secret information can be extracted completely from the carrier image.*

Keywords*-cryptography, hacking of information, edge, F5 Algorithm, mathematical morphology, Steganography*

I. INTRODUCTION

With digital cameras and digital scanners and other product since rise popularity , media applications, internet development and a variety of network multimedia information services widespread dissemination. Due to the ease in data communication the digital communication links are widely used nowadays however, the data transmitted through these links are insecure and prone to attacks. To communicate data secretly and to preserve information privacy is hence pivotal. Many different algorithm like Cryptography, Watermarking, Fingerprinting are used for the encryption of the information to be tranmitted. A new technology, Steganography, is the algorithm which hide the information behind the reference information. Small changes, which cant be detected by the human eyes at first sight, in the reference information gives advantages like a very high Security, extraction of the original information at receiver side, strong ability in anty-attack.

II. LITERATURE REVIEW

Steganography differs from cryptography[1],[2] in the sense that cryptography focuses on keeping the message secret while steganographt focuses on keeping the existence on the message secret. Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial.

Based on the multimedia used , the steganography can be classified into text, image, audio and video. Text Steganography hides the secret bits by formatting the ext or by encrypting the data using stego key. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

Image is composed of 8 bits per pixel i.e. 258 colours. The colours are generated from three primary colours namely red, green and blue (RGB). Various image steganography approaches have been designed in spatial and transform domain. Most commonly used spatial domain steganography approach is the LSB[4](Least Significant Bit) substituion technique. While JPEG[4] is the most commonly used technique into transform domain because of popularity on the Internet, and also of its small size. Video is nothing but collection of images with minor changes is frames in neighbourhood. Video means 50 images are pass through the human eye in one sec., such that the human eye cannot detect the differences in the images moving.

In the proposed method, hiding of text message behind a color image is shown. At first, from the color cover image, slices RGB is taken individually. All these slices are used to store the different information. After hiding of information these slices are again combined to make a color image which is to be transmitted, and which is nearly same as the original image.

The capacity of the hiding of information in the image is depend upon the edges of the image. The more the edgey image, the more capacity of hiding of information. We cannot hide much more information behid the cover image

though it has a high no of edges, because ressultant image should be nearly equal to original image and there must not be much more differences in between them. There are parameters like PSNR[5](Peak Signal to Noise Ratio) and MSE[5](Mean Square Error) are used to compare the stego images with there original images.

III. THE PROPOSED METHOD

The proposed steganography approach to improve the security is discussed in this section. Fig 1. Shows the flow of the proposed steganographic technique. The data encoding and decoding procedure are shown in this figure. The proposed algorithm is designed to embed text and image data into the video images. The embedding and extraction algorithm are discussed in detail.

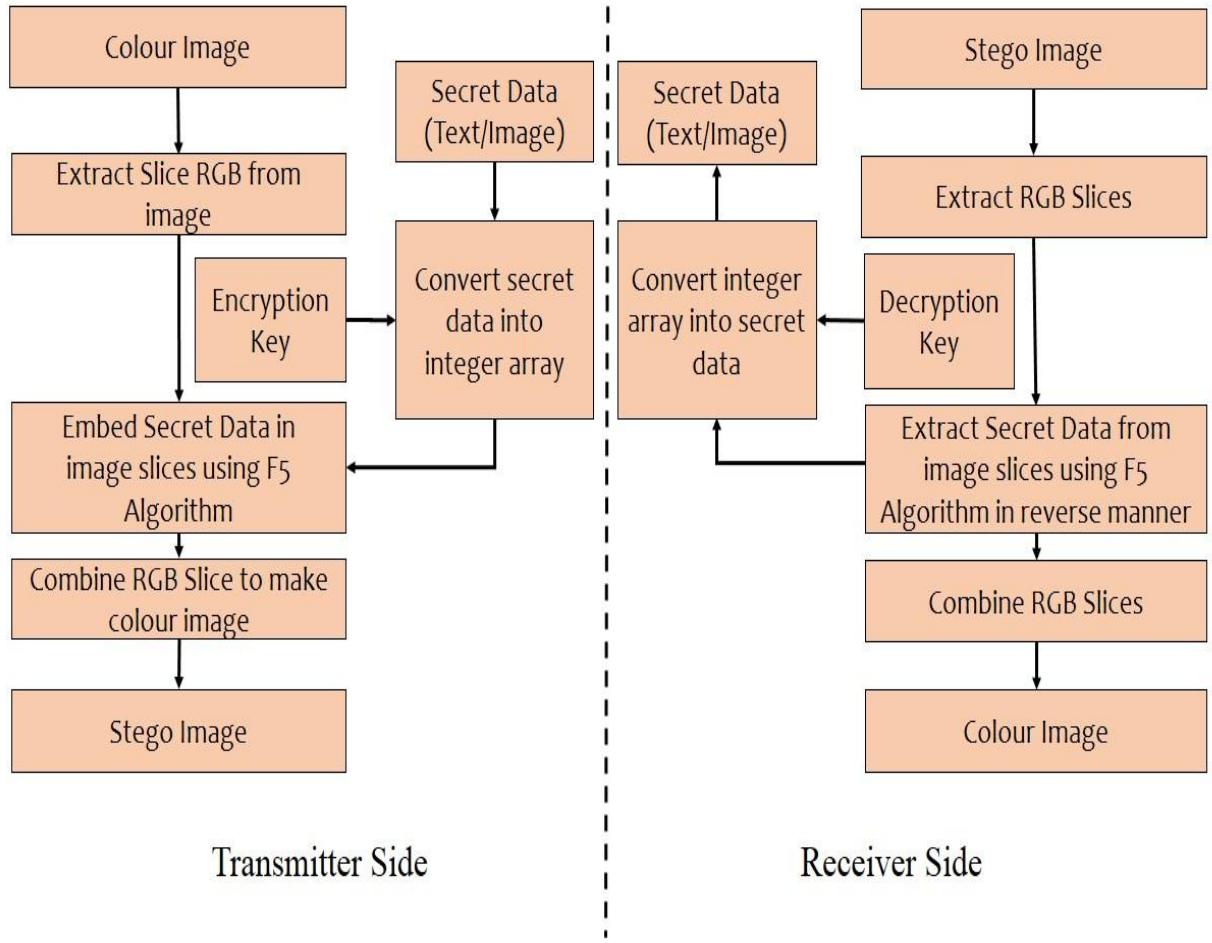

Fig 1. The Proposed Steganography System

Every pixel in a color image composed of three colors i.e. Red, Green and Blue. So, every pixel contains 24 bits (for 8-bit representation) where 8 bits for red component, 8 bits for green and 8 bits for blue component in a pixel. In proposed algorithm, slices of Red, green and Blue parts are extracted from the color image, and firstly Secret Data is embedded into Red slice, then in Green slice and then in Blue slice. Then, all this three slices are combined to generate Stego color image which is to be transmitted. The Embedding Algorithm is presented in section A and Extraction Algorithm is presented in section B.

A: EMBEDDING ALGORITHM

Inputs: Cover-Color Image, Encryption Key, Secret information
Output: Stego-Color Image

1. Read the text or image file that is to be hidden in cover-color image.
2. If Secret Data is in text format then convert it into ASCII format stream, and then convert this stream into binary form and go to step 4, otherwise go to step 3.
3. If Secret Data is in Image format, then extract three slices from it, make integer array of pixels in all of these three slices, and convert these secret data into ASCII format stream, and then convert this stream into binary form. Go to step 4.
4. Apply Encryption key in this Secret Data for the encoding of this Secret Data.
5. Apply F5 algorithm[3] to hide this secret data behind slices of the cover-color image.

6. Combine the slices to get Stego-color image to be transmitted.
7. Transmit the Stego-Color image.

B: EXTRACTING ALGORITHM

Inputs: Stego-Color Image, Decryption Key
Outputs: Cover-Color Image, Secret Information

1. Receive the Stego-Color Image.
2. Extract the slices from Stego-Color Image.
3. Apply inverse steps of F5 Algorithm to get the secret data from the slices of the image.
4. Apply Decryption key in this secret data for the decoding of the original information.
5. Now rearrange the information to get the Original text data (if it is), otherwise rearrange the data to get the slices of the image which is hidden.
6. Combine these Slices to get the original Hidden Information which is in Image format.
7. Now combine the Slices of the Color image to get the original Cover-Color image.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A: EVALUATION CRITERIA

The proposed algorithm is tested in MATLAB. In the proposed scheme both text and image data are used as secret data for data hiding. The performance of the proposed method is analyzed qualitatively. The proposed method is evaluated based on the Peak-Signal to Noise Ratio (PSNR) values and the distortion values using histograms of the cover-color images and stego-color images. PSNR is most commonly used parameter to measure the quality of images. PSNR is defined via the mean squared error (MSE). For two m×n images, cover-color image, C and stego-color image, S, the MSE is defined by using Eq.1 and PSNR is defined using Eq.2.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[C(i,j) - S(i,j)]^2 \quad (1)$$

$$PSNR = 10\,log_{10}\left(\frac{MAX_C^2}{MSE}\right) \quad (2)$$

Here, MAX_C is the possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented with B bits per sample, MAX_C is 2^B-1. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Table 1 shows the details of the sample cover-color images used for the demonstration of the proposed method and different secret messages used for data embedding. Fig 2 shows the different cover-color image.

a b c d

Fig 2. Cover-color images (a) Lenacolor.bmp (b) man.jpg (c) bullet.jpg (d) butterfly.jpg-Data Image.

a1 b1 c1

a2 b2 c2

Fig 3. Example of proposed steganography method. (a1) stego image-text.txt of 2(a); (b1) stego image-text.txt of 2(b); (c1)stego image-text.txt of 2(c); (a2)stego image-image.jpg of 2(a); (b2)stego image-image.jpg of 2(b); (c2)stego image-image.jpg of 2(c)

B: RESULTS

The changing level of the cover image that embedded information expressed by PSNR and MSE, table1 shows the change of PSNR and MSE that same secret information text.txt is embedded into different cover image. Stego images are shown in Fig 3[a1;b1;c1]. Table 2 shows the change of PSNR and MSE when the secret data is butterfly.jpg. Resultant Stego images are shown in Fig 3[a2;b2;c2]As we can see from the table, the same secret information being embedded into different cover image that have same size, the PSNR was in the same magnitude, does not appear the situation that too high or too low, also MSE was in the same magnitude. And if PSNR more than 32[3], it will not cause by the human eye's attention.

Table 1: Results of PSNR & MSE for different Cover-Images when Secret Data is text.txt

Image	PSNR	MSE
LenaColor.bmp	58.2761	0.0967
man.jpg	57.5733	0.1137
bullet.jpg	58.3932	0.0941

Table 2: Results of PSNR & MSE for different Cover-Images when Secret Data is butterfly.jpg

Image	PSNR	MSE
LenaColor.bmp	63.0473	0.0322
man.jpg	62.3445	0.0379
bullet.jpg	63.1644	0.0314

V. CONCLUSION

A random key based encoding and decoding in color images is proposed in this paper. The proposed method utilizes the encryption key to enhance the security of the system. The experimental results proved the quality of the video images are maintained well. From the results, it is concluded that the proposed method allows embedding of text data as well as Image data in the cover-color image. The hidden secret data is extracted without any errors.

VI. REFERENCE

[1] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." In Fifth Annual Information Security South Africa Conference, pp. 1-11. 2005.
[2] Yadav, Rajkumar. "Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters." International Journal of Computer Technology and Applications 2, no. 6 (2011).
[3] Gouxi, Chen, Cao Min, Fu Donglai, and Ma Qiaomei. "Research on a Steganographic Algorithm Based on Image Edge." In Internet Technology and Applications (iTAP), 2011 International Conference on, pp. 1-4. IEEE, 2011.
[4] Mandal, J. K., and Debashis Das. "Colour image steganography based on pixel value differencing in spatial domain." International journal of information sciences and techniques 2, no. 4 (2012).
[5] Ramalingam, Mritha, and Nor Ashidi Mat Isa. "A Steganography Approach over Video Images to Improve Security." Indian Journal of Science and Technology8, no. 1 (2015): 79-86.

