International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 06, June 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Image steganography technique to encrypt text data in Normal Image Space

Prof. C. G. Kokane Pawar, Prof. K. K. Nikam

[1,2]*Assistant Professor ,Sanjay Bhokare Group of Institutes Miraj,(India)*

Abstract

This paper proposed enhanced approach of image steganography forhiding text in Image Space. In the proposed encryption the message is inserted into the image with reference to a random generated key, using this key the extraction of text is done from the image. So this method is a highly secured from attack and highly complex to identify the text data in the image and retrieving the text message from the message is also a smooth process. The extraction is only possible when the key is known

Keywords: *Image steganography, pixel modification, steganography in spatial domain*

1. Introduction

As there is rapid advancement of the technology and science in nowadays there is an on-going need for new methods of information encryption is needed to secure one's private data. We are providing approach to this problem is to hide the secret information in public means of multimedia, popularly termed as steganography. Our Approach is to hide text message in an Image which is known as image steganography. This approach is composed with two steps, which areembedding and extraction with the help of a secret key. In the embedding process of "Image steganography technique to encrypt text data in Normal Image Space", the colour images are used as a non-secret means of multimedia, because a colour image can be represented in different colour models such as CMY colour model, HSI colour model, and so on….

This paper is based on RGB colour model because of its unique properties of colour representation of a colour pixel. The text message is embedded into the LSB of the binary Values of the colour component based on the secret key.

The Extraction process is quite simple &similar to the embedding process in which the message is retrieved on the bases of the modified secret key from the RGB's colour components of the modified image. This process is efficient enough that we can hide the text data at maximum of the size of the image, and the embedded data is stable enough that it is impossible to find the any difference between the original image and processed steganography image for naked eye.

Feifei [2] proposed a highly reliable face recognition algorithm using "Adjacent Pixel Intensity Differencing Quantization (APIDQ) histogram for face recognition" in spatial domain for this approach, Experimental results

show maximum average recognition rate of 97.2% for 400 images of 40 persons. Zhang's work [3] proposed an optimized EMD method by analysing the relation between n and payload in "Exploiting Modification Direction (EMD)", the pixels in the image are grouped into n pixels per group. A pixel in each group is modified one gray scale is at most to hide a secret digit in a (2n+1) binary notational system. Diwidisamidha's work discuss about the [4] various image steganography techniques in "Random image steganography in spatial domain", by considering pixel values in binary format and hide information in the spatial coordinates of the binary colour matrix. AliDaneshkhah [5] proposed "A more secure steganography method in spatial domain" presents an approach for hiding message in spatial domain. In this method two bits of the message is embedded in a pixel. S.G. Shelke [6] work discusses about different steganography schemes, its benefits and drawbacks are shown in the "Analysis of Spatial Domain Image Steganography Techniques".

Further paper is arranged as follows: Section II describes Image Steganography Techniques in Spatial Domain.In section III, the proposed image steganography algorithm is presented. Section IV presents the discussion on the experimental results and section V describes conclusions

2. Image steganography techniques in spatial domain

The steganography techniques can be classified into frequency/spectral domain techniques and spatial/substitution domain techniques.

Examples of some spatial domain techniques are, LSB method (Least Significant Bit) and PI method (Pixel Indexing). This proposed work is the enhancement of these techniques and used for image steganography process. Some brief of these basic techniques is given below.

LSB method (Least significant Bit): This method of steganography can be applied to both grayscale image and colour image. In this method of steganography the first step is to extract the RGB colour matrices from the image in the case of colour image, then the input text message is converted into the binary equivalent of the input string, and the next step is to embed the message into the least significant bits of the colour matrices with n-bits per pixel. Hence the embedding process is completed with the merging of these modified matrices.

The extracting process is as same as the embedding process, here we will separate the colour matrices from the stigno image and gathering all the n LSB bits pixel by pixel, then convert the concatenated binary values extracted from the matrices into its ASCII equivalents will give you the secret message embedded in the image.

PI method (Pixel Indexing): This method of steganography is only dedicated the colour image steganography, where the embedding process is composed of, Splitting the colour image into its colour matrices. In this method one of the colour matrixes is used as the key that indicates where the hidden message is embedded.

For example, the B (Blue component of the colour image) matrix is chosen as the reference matrix that indicates where the hidden message is embedded in the remaining two matrices.

Say, 1 0 1 0 0 0 1 0 is one of the binary converted pixel value of the B matrix. The least significant bits of the above pixel values are 1 and 0 indicating that the message is stored in the respective pixel of the R matrix and 0 indicates that no message has to be stored in respective G matrix. This process is repeated until the secret message ends.

The extraction process done by knowing the reference matrix and first and second matrix used for embedding, then the same process is repeated in reverse order and the extracted message is made concatenated in a temporary linear matrix and converted back into their equivalent ASCII values, hence the secret message is extracted. Even though the embedding process is little tricky but the probability of finding the correct method is so high, that means it is vulnerable to attacks.

So, we proposed a better and efficient method for Text Embedding Image Steganography which is complex to find and retrieve the message. Our method of steganography is explained below.

3. Proposed work

The process of embedding and extracting the text message into an image and from an image is shown with a keen algorithm shown in below.

Algorithms embedding algorithm

STEP 1: Take a colour image as input.

STEP 2: Split the colour image into RGB components.

STEP 3: Convert decimal RGB matrices into binary matrices.

STEP 4: Take a text message to embed into the colour image.

STEP 5: Convert text message into its equivalent binary values.

STEP 6: Generate a binary Key matrix with three columns and same number of rows in a binary colour matrix.

STEP 7: If '1' is encountered 1. Embed (first/next) 3 bits of message into LSB in the respective dedicated colour matrix. 2. Move to next bit in the key. 3. Go to Step 7 Else 1. Move to the next bit in the key. 2. Go to Step 7 The above process is repeated until the message is end.

STEP 8: Convert modified colour matrices back to decimal values.

STEP 9: These modified RGB colour matrices is merged to form the Stigno image.

Extracting algorithm

STEP 1: Stigno image as input.

STEP 2: Extract RGB values from the modified colour image.

STEP 3: Convert decimal colour matrices into binary matrices.

STEP 4: Get the embedded binary key.

STEP 5: If '1'is encountered

1. Get 3 bits from the corresponding colour matrix to the empty string.

2.Move to the next bit in the key.

3. Go to STEP 5.

ELSE 1. Move to the next bit of the key.

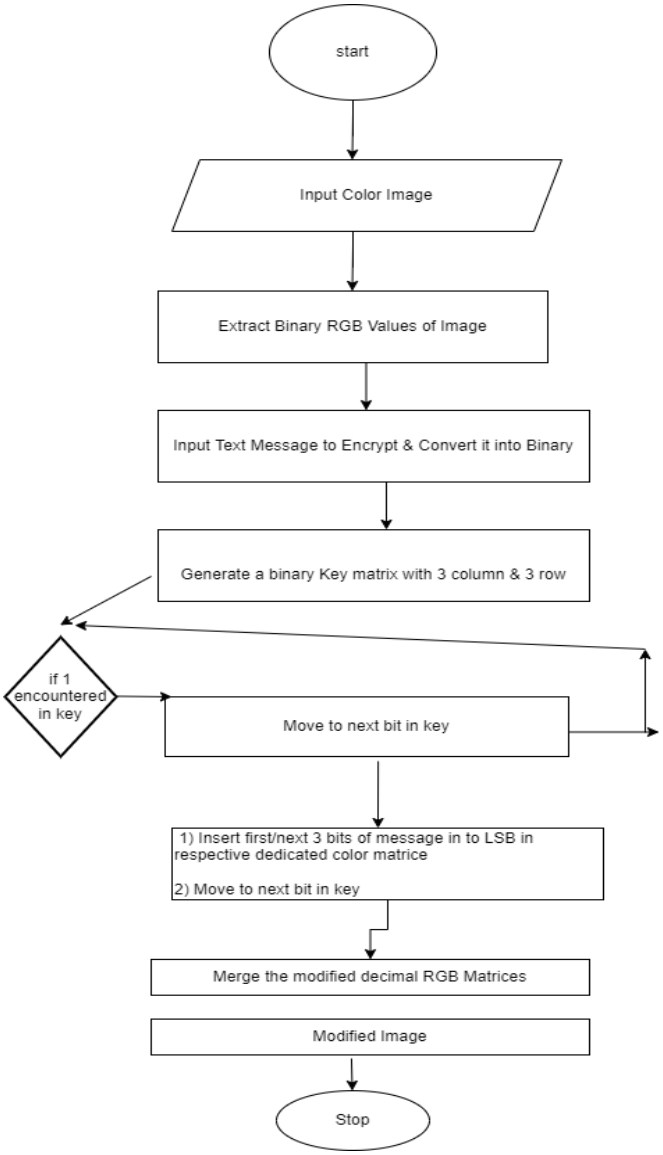
2. Go to STEP 5 Repeat this process until the key ends.

STEP 6: Resulting string is the extracted message.

NOTE: Here the binary key generated is a randomly generated key; this key generated will never be same no matter how many times you run the code it will generate a new key again and again.

2. Flow charts

Embedding flow chart



Extracting algorithm

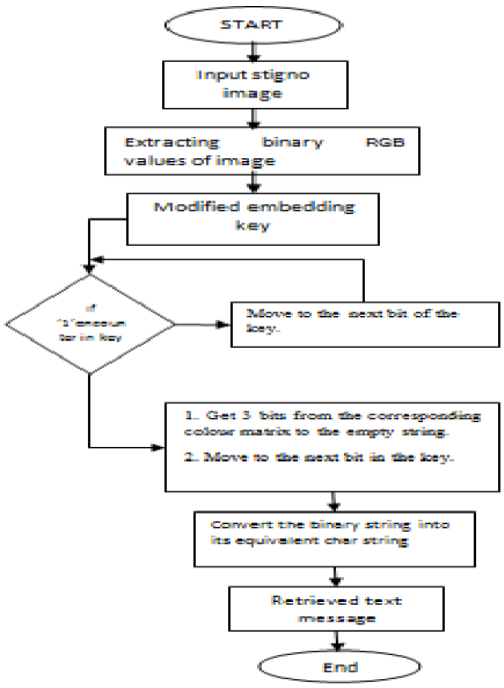


Fig. 3: Flow chart of proposed work for text extraction

4. Experimental results

For the simulation we have used the latest version of the mat lab. For the execution of proposed work the size of the cover image is 200 × 250.Now embedding & extraction of the proposed work has been done on the cover image and a text message is taken as input. The different cases are shown in below

CASE 1

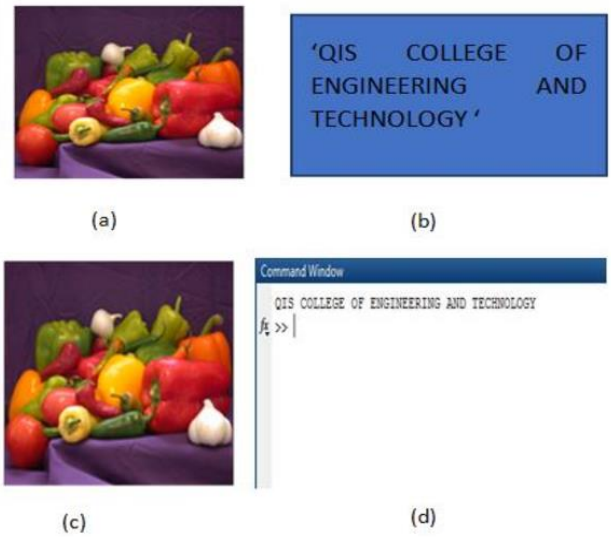


Fig. 3: (a) Input image (b) input message (c) stignoimage, (d) extracted

Fig. 3: (a) Input image (b) input message (c) stignoimage, (d) extracted message

CASE 2

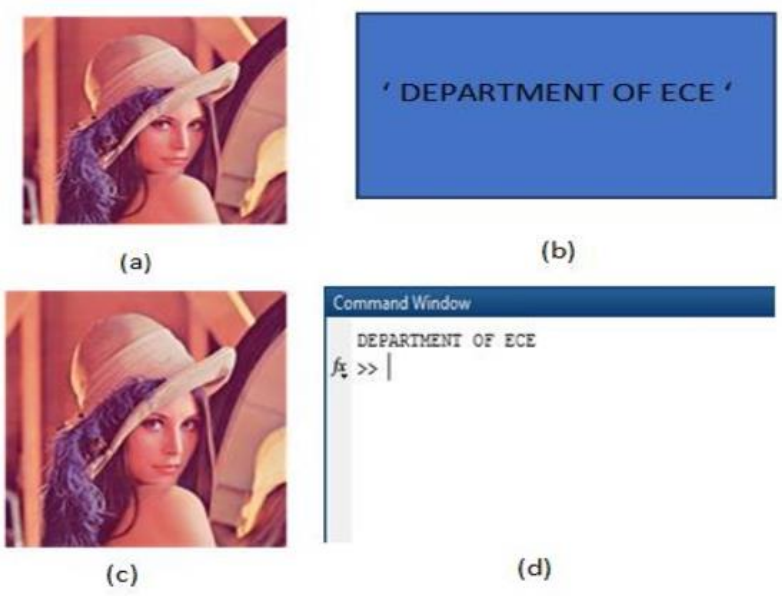
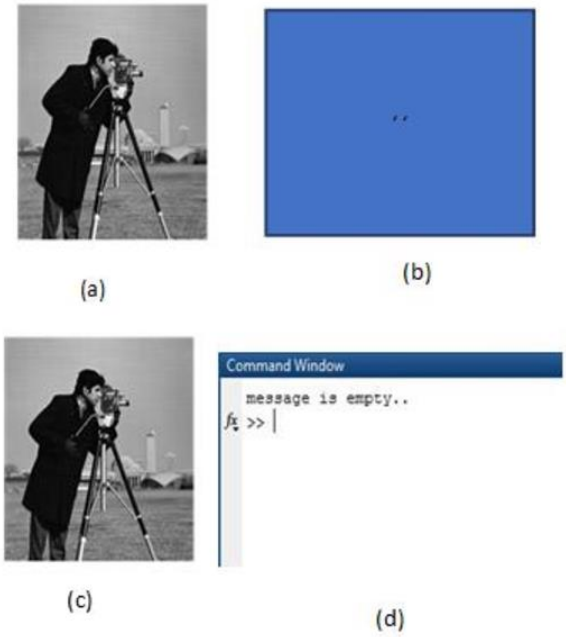


Fig. 4: (a) input image (b) input message (c) stignoimage, (d) extracte

CASE 3



'ig. 5: (a) input image (b) input message (c) stignoimage(d) extracted message

5. Conclusion

In this project it has been shown that the steganography concepts and modified pixel indexed technique to images, the robustness of the steganography has been quantitively measured by comparing the extracted

embedded image with the original. The absolute differences between the original and modified image are found out tough to identify.

The theme of the proposed project is beneficial to carry secret messages in non-secret photograph. So that the information security has been improved. This thing can also be applied in the sectors where high confidentiality is required, here it is complex to extract the encrypted file. The sectors in which it can be applied are, Banking, Hospitals, Police Department, etc.

6. References

[1] Gonzalez RC & Woods RE, Digital image processing, Pearson 3rd edition, (2008).

[2] Lee F &Kotani K, "Face Recognition Using Adjacent Pixel Intensity Difference Quantization Histogram Combined with Markov Stationary Features", International Journal of Advancements in Computing Technology (IJACT), Vol.4, (2012).

[3] Zhang X & Wang S, "Efficient steganographic embedding by exploiting modification direction", IEEE Communications Letters, Vol.10, No.11,(2006).

[4] Samidha D &Agrawal D, "Random image steganography in spatial domain", International conference on Emerging trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), (2013), pp.1-3.

[5] Daneshkhah A, Aghaeinia H &Seyedi SH, "A more secure steganography method in spatial domain", Second International Conference on Intelligent Systems, Modelling and Simulation (ISMS), (2011), pp.189-194.

[6] Shelke SG &Jagtap SK, "Analysis of Spatial Domain Image Steganography Techniques", International Conference on Computing Communication Control and Automation, (2015)