INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume3, Issue2)

Available online at www.ijarnd.com

Data Hiding Using Image Steganography

Nannapaneni Manoj Kumar[1], M.Praveen Kumar[2], M.Srinivasa Rao[3]

[1] *Student, ECE, VVIT, Andhra Pradesh, India*
[2] *Student, ECE, VVIT, Andhra Pradesh,India*
[3]*Assistant Professor,ECE, VVIT, Andhra Pradesh, India*

ABSTRACT

Data security is the most concerned factor in the era of vast technical advancement. Vast technical knowledge paved a path for the evolution of data-stealing techniques. Steganographic techniques help to mask the secretive information with some other media that acts as a cover to the information. This technique makes it very difficult for hackers to notice the information because it appears in form of a media rather than as information itself. The media file can be an audio, image or a video. Image steganography helps to hide secret information in images. These images can be exchanged without seeking any attention of hackers to the secret information inside it. The information is encrypted before embedding it into the image, to make it safer. This can be decrypted at the receiver side with proper algorithm along with a correct key.

This project involves encrypting the information and hiding it in the image using LSB array. Extracting the information and decrypting it is done at the receiver.

Keyword: *Steganography, Encryption, Decryption, LSB Array.*

1. INTRODUCTION

Information security is a most concerned factor in a communication system. Especially confidential information being exchanged should be much safer from hackers and cyber-attacks. This can be achieved by exchanging the information by making it visible as a media i.e. audio, image or video etc. This technique of using a media to mask the information is called steganography. The word 'Steganography' is of Greek origin and it means 'covered writing'. This technique has been in use from a very ancient time. Earlier, chemicals were used on paper to make the letters invisible. These letters are seen by heating the paper. There is a wide difference between encryption techniques and steganographic techniques. An intruder can sense some information is being transmitted by observing the encrypted text, but he cannot decrypt it with a correct key. Whereas an intruder cannot even sense that information is being exchanged if steganographic techniques are used. This paper proposes a steganographic technique used on encrypted information. So it will be almost impossible for intruders to extract the information. Steganography can take many forms such as audio steganography, image steganography and video steganography. This paper will focus mainly on image steganography. Image steganography can be implemented using many algorithms but LSB array modification is most flexible and efficient among them all.

1.1 Image Steganography

Information can be hidden in an image by embedding the characters of the information into the pixels of the image. A pixel is a basic color unit of an image. These pixels are placed next to each other to obtain an image. Each pixel has its own intensity value. This intensity value decides visual appearance of that particular pixel. The intensity of each pixel is stored in form of a positive integer value. The range of this integers depends on the type of image i.e. A Black and White image can have a pixel value either zero or one, a Grey scalehas pixel values ranging from 0 to 255, in color images each color component has pixel values ranging from 1 to 255. The Least Significant Bit(LSB) of these integers usually carry less information. Though, the LSB of the pixel's intensity value has changed the change in the appearance of the pixel cannot be noticed by the human vision. More than one LSB bit can be changed till the visual appearance of that pixel is not affected. i.e. an LSB array can be modified instead of a single LSB bit. This principle is the basic key to hide the information. The information can be hidden in the one or more Least Significant Bits of the pixels. The visual appearance of the image is not affected. This technique does not need transform domain operations. It can be carried out in the spatial domain. So it is more simple and flexible. In transform domain, it requires manipulation of complex algorithms.

2. LITERATURE SURVEY

Paper: "Improvement in Image Steganography by LSB inversion method- A Case Study", 2017-INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH (IJITR).

Author: Ms. A. S. Bhandare, Padmabhooshan Vasantrodada Patil Institute of Technology, Budhgaon. Maharastra, India.

Description: "In this mentioned system only one bit from a pixel is used to store the information available. A character contains 8 bits of information. So it takes 8 pixels of the image to store one character information. So the number of characters that can be stored in an image is very less i.e. Number of pixels/8. In the currently proposed system, color images are used to hide the information. In colorimages, each pixel has three components i.e. Red, Blue and Green as a vector space as shown in Fig.1.

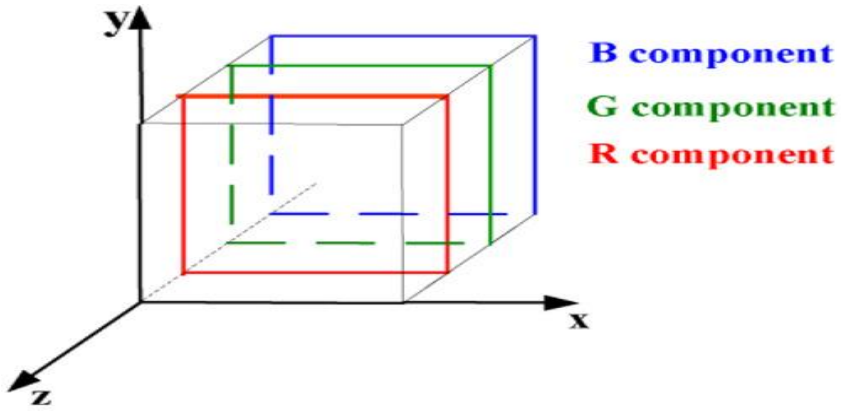

Fig.1: RGB Vector Space

Each component is represented by 8 bits. Three LSB bits from each color component are used to store the information. So nine bits are available from each pixel to store the information. One character can be stored in one pixel. So total number of characters that can be stored in the image are equal to the total number of pixels in the images. The quality of image is not affected by this approach. So the redundancy bits are used more efficiently and the capacity of storing the information is improved 8 times the previous system."

3. ABOUT MATLAB

MATLAB is a Multi paradigm numerical computing environment. It is a proprietary programming language developed by Math Works. Matlab allows Matrix Manipulations. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. The MATLAB working environment provides a set of tools and facilities to work with. It includes facilities for managing variables in the workspace, importing and exporting data. It also includes tools for developing, managing and debugging. Matlab also supports various languages like C, Cpp, Java, FORTRAN, Python, etc. Matlab code complier helps to convert the Matlab code to any other language.

MATLAB Graphics system includes high-level commands for two dimensional and three-dimensional data visualization, image processing, animation and presentation graphics. It also includes low-level commands that allow to fulfill customize the appearance of graphics as well as to build complete Graphical User Interface on Applications.

3.1. Matlab Image Processing Tool Box

Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and workflow apps for image processing, analysis, visualization, and algorithm development. You can perform image segmentation, image enhancement, noise reduction, geometric transformations, image registration, and 3D image processing.

Image Processing Toolbox apps let you automate common image processing workflows. You can interactively segment image data, compare image registration techniques, and batch-process large datasets. Visualization functions and apps let you explore images, 3D volumes, and videos, adjust contrast, create histograms, and manipulate regions of interest.

4. IMPLEMENTATION

The flow of implementation is shown in Fig.2. The message file containing the information should be selected by the user to start. This can be a file in any of the various formats like .txt, .doc, etc. The information can also be manually typed by the user. The information from the file is stored in a variable in theworkspace. In its next step, the information needs to be encrypted with any of the available encryption techniques using a proper key. The purpose of encryption is to generate a cipher text from plain text. Plain text is the information we provide directly. This information can be easily understood by the intruders if they look into it. But the cipher textdoes not have any meaning. It cannot be understood by any one by observing it. It can only be understood after decrypting it using a correct key.

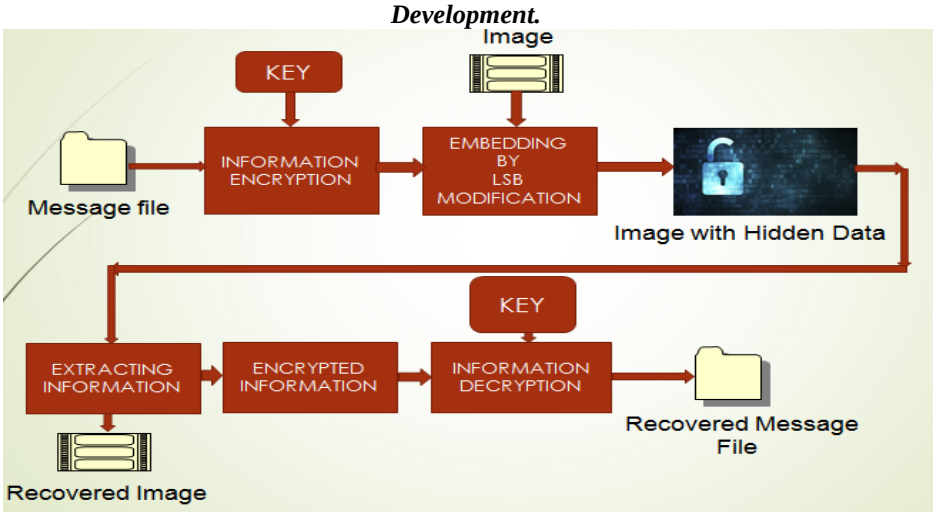

Fig.2: Implementation Flow Diagram

The next step to encryption is embedding the encrypted cipher text into the image using the LSB modification technique. A cover image should be selected by the user to embed the cipher text into it. To embed the cipher text into the image, each character is selected and its bit format is produced. These bits are replaced at the last three LSB positions of Red, Green and Blue components of the pixel.

Consider a pixel with Red component equal to 11011010 and Green component equal to 10110111 and blue component equal to 11110010. Let the ASCII value of the current character being embedded be 11001101. Now the LSB bits of Red, Green,and Blue components are changed as 11011**110**, 10110**011** and 11110**01** respectively. The first three MSB bits of the character are replaced at the last three LSB bits of the Red component. The next three bits of the character are replaced at the last three LSB bits of the Green component. The remaining two bits of the character are replaced at the last two LSB bits of the blue component. In this manner, one character is embedded into the LSB positions of the three components of a single pixel. This process is done till all the characters of the information are embedded into the pixels of the image. There is a major constraint on the number of characters that can be embedded in this process. The number of characters that can be embedded cannot exceed the total number of pixels in that image. So images with higher resolution should be used in order to hide more number of characters.
Once the embedding process is completed the image containing the hidden data is generated. Visually, it is impossible to notice any difference between the original image and the image with hidden information. So this image can be exchanged over a medium without seeking any attention from hackers and intruders. The major constrain here is the medium over which the image is being transmitted should not affect or disturb the image. i.e. The physical size or resolution or any other factor of the image should not be processed or affected by the medium.

At the receiver, the information from the received image should be extracted in the first step. The LSB bits of the three components of the pixel should be brought together to obtain the character embedded into that pixel. For example, if the Red, Green and Blue components of a received pixel are 11011110, 10110**011** and 11110**01** respectively. Then the character embedded into that pixel is 11001101. This is extracted by putting the three LSB bits of Red component and three LSB bits of Green component and two LSB bits of Blue component together. This need not be the exactly same pattern to be followed. The components can be used in any order during embedding. The last three LSB bits can also be used in any order to replace the character bits.

After extracting the characters from the image the generated text is the cipher text. This cipher text should be converted back to the plain text to recover the original message information. The decryption algorithm should be run on the cipher text using a correct key to get back the plain text. Using a correct key can only generate the correct information. An incorrect key generates an incorrect and meaningless information**.**

5. RELATED WORK

The original image used for embedding the information can be seen in Fig.3. The image obtained after performing steganography, called the stego image contains the hidden information and it can be seen in Fig.4. We can observe that there is no visual difference between those two images. They appear exactly the same in appearance but there is hidden information in the image we see in Fig.4.

Fig.3: Original Image without Information

Now the encrypted information is embedded into this image using the LSB modification algorithm to obtain the image with that information. The image with information hidden into it is obtained and is shown in Fig.4.

Fig.4: Stego Image with Information

The recovered image after extracting the information also looks exactly the same like the original image as in Fig.3. So the information is obtained without disturbing the visual appearance of the original image used by the user.

6. CONCLUSION

This paper presents the Information hiding using Steganography. It is the right technique to exchange secret information over the internet. In particular, LSB modification technique has been keenly discussed. The major advantage of this technique is its flexibility and efficiency. Another added advantage is that is a spatial domain technique. There is no need to remember complex transform domain algorithms. Image steganography technique can be used to save important passwords and keys without visibility to the external world. It can also be used by the digital art makers to protect the copy rights of their digital arts by embedding their details into the work.

7. REFERENCES

[1]https://www.researchgate.net/publication/262488507_Steganalysis_Detecting_LSB_Steganographic_Techniques
[2]https://www.sciencedirect.com/science/article/pii/S1047320310001161
[3]https://ac.els-cdn.com/S2212667813000075/1-s2.0-S2212667813000075-main.pdf?_tid=3b246906-0a24-11e8-ac76-00000aacb361&acdnat=1517801316_ea29948af00da9d37f0d629e7f4aa423
[4]http://www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/lsb.html
[5]https://www.tutorialspoint.com/matlab/matlab_data_import.htm
[6] https://in.mathworks.com/matlabcentral/answers/86410-changing-values-of-pixels-in-an-image-pixel-by-pixel-thresholding
[7]https://in.mathworks.com/matlabcentral/answers/60261-how-to-change-least-significant-4-binary-bits-of-each-bit-of-cover-image-by-other-four-b

