Encoding and Decoding of Image using Steganography Technique

Manjit Sandhu, Jaipreet Kaur, Sukhdeep Kaur
Assistant Professor, Department of ECE, GNDU Regional Campus, Sathiala Amritsar, India.

Abstract-**The work is primarily concentrated on the data security issues while sending the data over the network using steganographic techniques.This paper is an overview encoding the image using Steganography which is art and science of writing hidden messages in such a way that no one apart from the sender and the intended recipient can realize that hidden data. Firstly the binary representations of hidden data are taken and then overwrite the LSB of each byte within the cover image and get the encoded image i.e. cover image with message image. Then from histogram of cover, message and encoded images respectively difference between original cover and encoded image is made clear. At the last extraction of message image from encoded image is done by shifting the bits in opposite direction. This shows that steganography is simplest method which provide privacy and secrecy both in case of hiding image within image.**

Index Terms— **encoding, decoding, encryption, decryption, RGB**

1. INTRODUCTION

The word steganography is of Greek origin and means "covered, or hidden writing". Steganography is the art and science of communication in such a way which hides the existence of the communication. This can be achieved by concealing the existence of information within seemingly harmless carriers or cover. The first recorded use of steganography can be traced back to 440 BC when Herodotus mentions an example of steganography in the histories of Herodotus .Example is that of histories, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the Persians. During the "Cold War" period, U.S. and USSR wanted to hide their sensors in the enemy's facilities. These devices had to send data to their nations, without being spotted. In October 2001, the New York Times published an article claiming that al-Qaeda had used steganography to encode messages into images, and then transported these via e-mail and possibly via USENET to prepare and execute the September 11, 2001 terrorist attack.

2. STEGANOGRAPHY AND CRYPTOGRAPHY

2.1Pure steganography

Pure steganography is the process of embedding the data into the object without using any private keys. This type of steganography entirely depends upon the secrecy. This type of steganography uses a cover image in which data is to be embedded, personal information to be transmitted, and encryption decryption algorithms to embed the message into image.

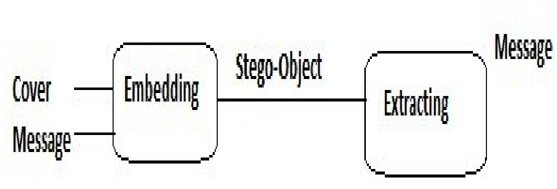


Fig.1 Block diagram of steganographic technique

2.2Cryptography — the science of writing in secret codes/addresses all of the elements necessary for secure communication over an insecure channel, namely privacy, confidentiality, key exchange, authentication, and non-repudiation. But cryptography does not always provide safe communication. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. Whereas the goal of cryptography is to make data unreadable by a third party , the goal of steganography is to hide the data from a third party. Often, steganography and cryptography are used together to ensure security of the covert message.

3. ANALYSIS OF DIGITAL IMAGE

An image file is merely a binary file containing the binary representation of the color or light intensity of each picture element (pixel) comprising the image.Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pixel is represented by three bytes, each byte representing the intensity of the three primary colors red, green, and blue (RGB), respectively.

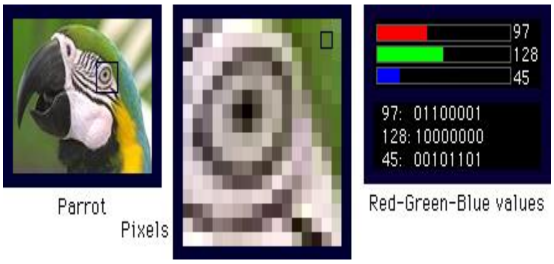


Fig2. Image ,its pixels and its RGB values

4. LEAST SIGNIFICANT BIT INSERTION (LSB)

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the cover image. It is a simple approach for embedding message into the image. In this project clearing of cover image LSB bits is done .Then message image MSB bits are moved at place of LSB bits To do this we use matlab commands which are :

1. bitand = performs bitwise and operation
2. bitshift = perform bit shifting

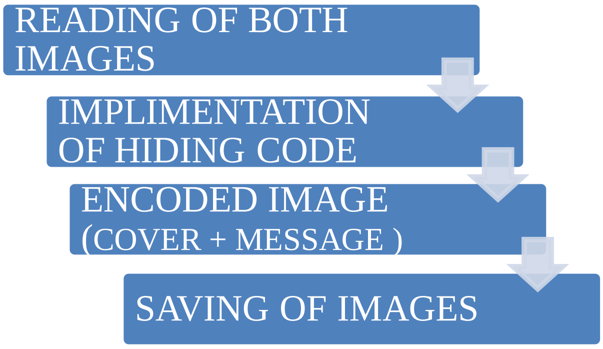
The simplest approach to hiding data within an image file is called LeastSignificant Bit (LSB) insertion. In this method, we can take the binaryrepresentation of the hidden data and overwrite the LSB of each byte within thecover image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data

is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed):

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.



READING OF BOTH IMAGES

IMPLIMENTATION OF HIDING CODE

ENCODED IMAGE (COVER + MESSAGE)

SAVING OF IMAGES

Fig 3. Block diagram for hiding data

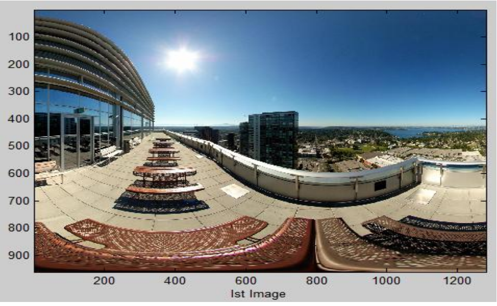


Fig.4. Cover Image

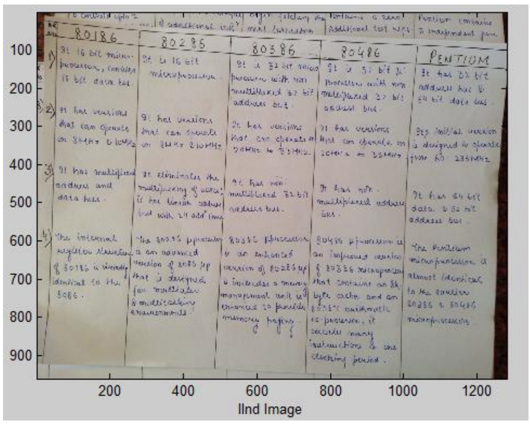

80186
80286
80386
80486
PENTIUM
100
200
300
400
500
600
700
800
900
200
400
600
800
1000
1200
IInd Image

Fig.5. Message Image

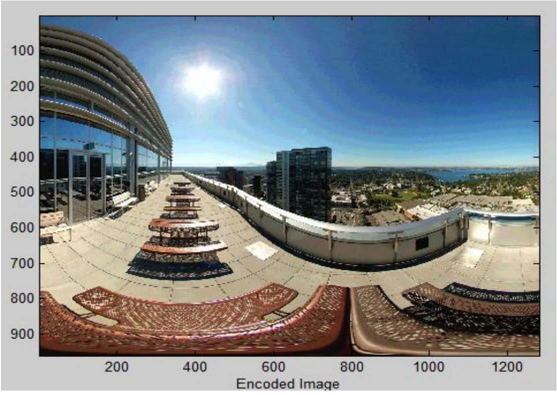


Fig 6 Encoded image

5. HISTOGRAM CHECKING METHOD

A histogram is graphical representation of the distribution of numerical data . it is an estimate of probability distribution of continous variable and was first introduced by karl pearson.The histogram of the digital image is a graph plotting the number of pixels with the specific gray level versus the gray level value .

RESULTS OF HISTOGRAM:

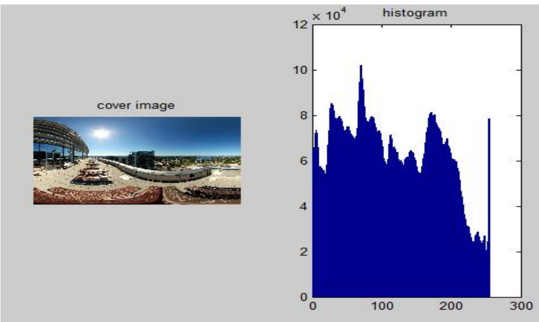


Fig.7 Histogram of cover image

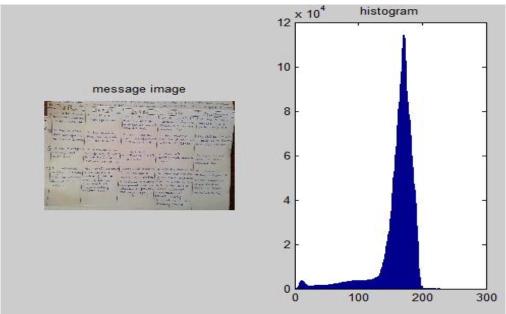


Fig.7 Histogram of message image

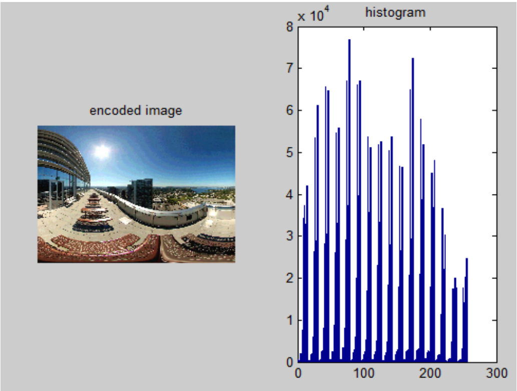


Fig.7 Histogram of encoded image

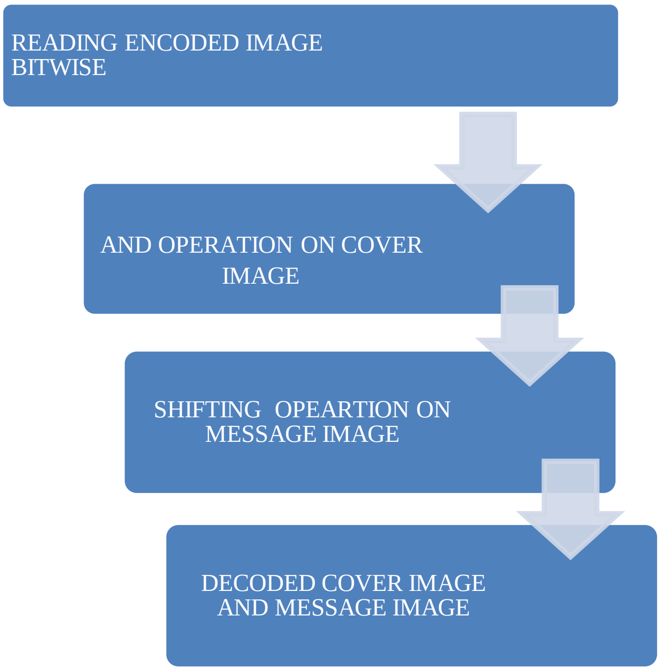

READING ENCODED IMAGE BITWISE
AND OPERATION ON COVER IMAGE
SHIFTING OPEARTION ON MESSAGE IMAGE
DECODED COVER IMAGE AND MESSAGE IMAGE

Fig 8 Block diagram explaining matlab code

6. RESULTS

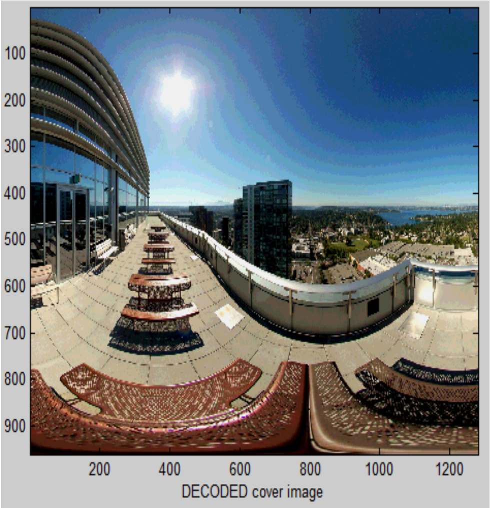


Fig 9 Decoded cover image Decoded covered image

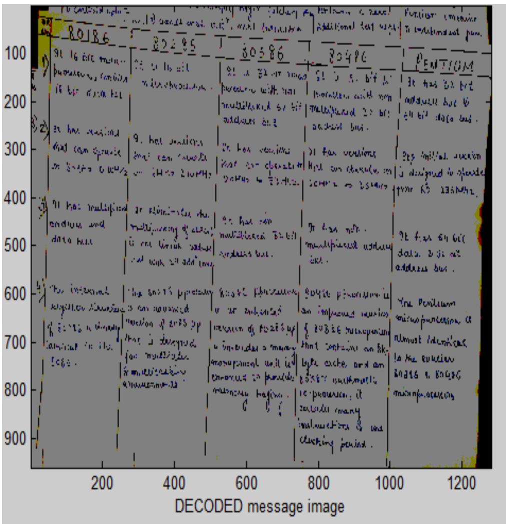


Fig 9 Decoded cover image Decoded message image

5. CONCLUSION

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to user. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected. Steganography is still a fairly new concept to the general public although this is likely not true in the world of secrecy and espionage. Digital watermark technology is currently being used to track the copyright and ownership of digital content. Efforts to improve the robustness of the watermarks are necessary to ensure that the watermarks and embedded information can securely defend against watermarking attacks. With continuous advancements in technology it is expected that in the near future more efficient and advanced techniques in steganalysis will emerge that will help law enforcement to better detect illicit materials transmitted through the Internet. The tutorial introduces a tiny part of the art of steganography. Steganography goes well beyond simply hiding text information in an image. Steganography applies not only to digital images but to other media as well, such as audio files, communication channels, and other text and binary files.

6. REFERENCES

[1]. Amirthanjan,R. Akila,R & Deepika chowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application.

[2]. Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in Technology.

[3]. Cox, I. Miller, M. Bloom, J. Fridrich, J & Kalker, T. 2008. Digital watermarking and Steganography.2ndEd. Elsevier.

[4].Obaida Mohammad Awad Al-Hazaimeh Hiding Data in Images Using New Random Technique Department of Information Technology, AL-BALQA Applied University/Al-Huson University College, Irbid, Al-Huson, 50, Jordan.

[5].An Overview of Steganography by Shawn D. Dickman Computer Forensics TermPaper, James Madison University.

[6].A Tutorial Review on Steganography by Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjeet and Poulami Das University of Calcutta.

[7].Exploring Steganography: Seeing the Unseen by Neil F. Johnson Sushil Jajodia George Mason University.