IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

A Secure Data Hiding Scheme For Color Image

Mrs. S.A. Bhavani

Assistant Professor, Department of Computer Science and Engineering, Anil Nerukonda Institute of Engineering and Technology, Sangivalasa, Visakhapatnam, AP, India

Abstract: Any information stored in a computer needs to be kept secret from the outside users as they may use the data for illegal purposes. In order to achieve this security, we propose a new Steganography scheme for hiding a piece of critical information in a host binary image. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. There are three basic types of Steganography: Image, Text and Audio/Video. Steganography is the science which deals with security issues. It refers to the art and science of writing messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Main goal of steganography is to protect data from unauthorized users. The two key processes used in Steganography are: Encryption and Decryption. In this paper we use a secret key and a weight matrix to protect the hidden data. Given an image block of size m x n, our scheme can hide as many as $\log_2(mn+1)$ bits of data in the image by changing at most 2 bits in the image. This scheme can provide highest security, embed more data and maintain higher quality of the host image. The project evaluates the performance of the above mentioned algorithms and suggests the best suitable technique from the comparative study of images. In this paper we have presented a new steganography scheme for hiding critical information in a host binary image. The main idea is to use a secret key and a weight matrixto protect the hidden data and maintain higher quality of the host image. Our scheme is to use the best technique available to provide a higher data hiding ratio, but change less pixels in the original image.

Keywords: Steganography, spatial domain, transform domain, LSB, PVD.

1. INTRODUCTION

Information stored in a computer must be kept secured against unauthorized access of outside people. The possibility that the information stored in a personal computer or the information that is being transferred through network of systems or computer or internet being read by any other people is very high. As digital media are getting wider popularity, their security- related issues are becoming a great concern. One central issue is confidentiality, which is typically achieved by encryption. However, as an encrypted message usually flags the importance of the message, it also attracts cryptanalysts' interests. The sometimes confusing terminology stagenography has a different flavor from encryption; its purpose is to embed a piece of critical information in a non-critical host message (e.g., webpages, advertisements, etc.) to distract opponents' attention. One less confusing name for steganography would be data hiding. It should be understood that steganography is orthogonal to encryption, and it may be combined with encryption to achieve a higher level of security.

Data hiding is usually achieved by alternating some nonessential information in the host message. Given a color image, one simple approach is to use the least-significant bit (LSB) of each pixel to hide information. As this is not likely to degrade the quality of the image, a number of software packages have adopted this approach. A more challenging problem is to hide data in a two-color binary image (e.g., black-and-white images, such as facsimiles and bar codes). The reason is that changing a pixel can be easily detected.

It is to be noted the digital image watermarking technology has a different flavor from what is to be discussed in this paper. Its purpose is to embed some ownership or authentication information in an image. It is usually desirable to make a watermark visible to a certain degree, instead of completely hidden, to claim the ownership of an artwork. For all the above problems we must need an efficient security providing technique i.e Steganography is used in our project to protect the data from un-authorized access.

1.1 DATA HIDING TECHNIQUES:

Information hiding techniques are broadly classified into four categories such as, Covert channels, Steganography, Anonymity and Copyright marking.

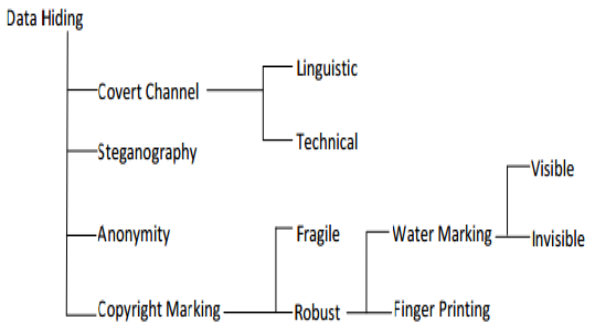


Fig.4. Data hiding techniques

DOI 10.17148/IJARCCE.2016.5845

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

The Steganographic procedures can be linguistic or technical whereas the copyright marking procedures can be robust or fragile. Watermarking is a type of robust copyright marking technique which can further be classified as perceptible or imperceptible watermarking. The figure below gives a complete classification of various data hiding techniques.

1.2 WHAT IS STEGANOGRAPHY? :

Steganography is the practice of concealing messages or information within other non-secret text or data. The word steganography combines the Greek words steganos, meaning “covered, concealed, or protected", and graphein meaning "writing". The purpose of steganography is to maintain secret communication between two parties.

The basic structure of Steganography is made up of three components: the carrier, the message, and the key. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will ‘carry’ the hidden message. A key is used to decode/ decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light.

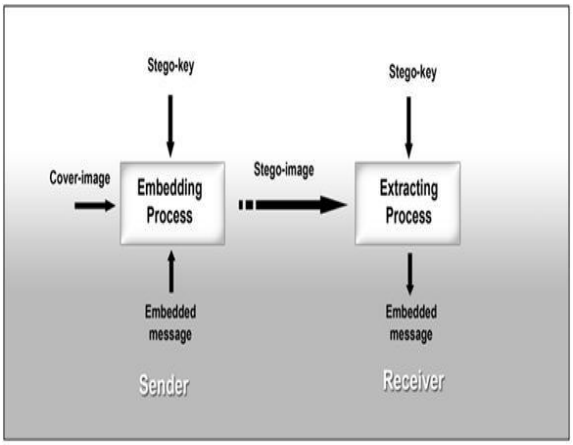


Fig: 1 Steganography Classification

Depending upon this carrier file, steganography is classified as:

(i) TEXT STEGANOGRAPHY

In text steganography formatting or by changing certain characteristics of textual elements can be changed. It consists of line-shift coding, word-shift coding and feature coding.

(ii) IMAGE STEGANOGRAPHY

In this steganography, image is commonly used cover file. There are different file formats are available for digital images and for these file formats different algorithms are exist such as least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

(iii) AUDIO STEGANOGRAPHY

In audio steganography, secret message is embedded into digitized audio signal which result slender shifting of binary sequence of the equivalent audio file. There are a number of methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

(iv) VIDEO STEGANOGRAPHY

Video files consist of assortment of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. Advantages of using video steganography are that large amount of data that can be hidden inside the cover file and it is the fact that it is flow of images and sounds.

1.3 ENCRYPTION AND DECRYPTION:

ENCRYPTION:

It is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted.

DECRYPTION:

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

1.4 PRINCIPLES OF SECURITY:

In order to achieve security, we must follow the basic principles of security. The basic principles of security help in transmitting the data more efficiently and securely. The four basic principles of security are Confidentiality, Integrity, Aunthentication and Non- Repudiation. The access control and availability also come under principles of security. In this project confidentiality is the central issue and this can typically achieved through encryption.

CONFIDENTIALITY:

This is the first basic principle of security which deals with the access of the data by the right persons. The

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

principle of confidentiality mentions that only the sender and the intended recipient should be able to access the data transmitted over the network. If any other persons access the data, the principle of confidentiality gets compromised. So in order to achieve security we must protect the data from unauthorized access.

1.5 WHAT IS IMAGE PROCESSING?

Image processing is a method which includes some operations to be performed in order to convert an image to get an enhanced image or to extract some useful information from it. The input is an image like a photograph or video frame
whereas the output may be an image or characteristics related to the image.

1.6 APPLICATIONS OF STEGANOGRAPHY:

Steganography is applied in the following areas:
1) Confidential communication and secret data storing.
2) Protection of data alteration
3) Access control system for digital content distribution.
4) Media Database systems.

1.7 KEY PROPERTIES OF DATA HIDING:

A few key properties that must be considered when creating a digital data hiding system are:

• IMPERCEPTIBILITY:
Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image.

• EMBEDDING CAPACITY:
Refers to the amount of secret information that can be embedded without degradation of the quality of the image.

• ROBUSTNESS:
Refers to the degree of difficulty required to destroy embedded information without destroying the cover image.

1.8 STEGANOGRAPHY TECHNIQUES:

1.8.1 CLASSIFICATION OF STEGANOGRAPHIC CATEGORIES

Steganography is classified into 3 categories-
• Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
• Secret key steganography where the stego key is exchanged prior to communication. This is most suspectible to interception.
• Public key steganography where a public key and a private key is used for secure communication.

1.9 CLASSIFICATION OF STEGANOGRAPHIC METHODS

Steganography methods can be classified mainly into six categories, although in some cases exact classification is not possible.

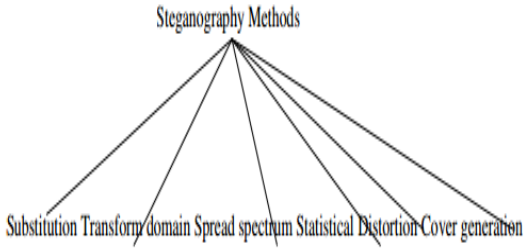


Fig:2 Classification of Steganographic methods

• Substitution methods substitute redundant parts of a cover with a secret message (spatial domain).
• Transform domain techniques embed secret information in a transform space of the signal (frequency domain)
• Spread spectrum techniques adopt ideas from spread spectrum communication.
• Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
• Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.
• Cover generation methods encode information in the way a cover for secret communication is created.

2. EXISTING STEGANOGRAPHIC TECHNIQUES

The steganographic algorithms proposed in literature can broadly be classified into two categories:
1. Spatial Domain Techniques
2. Transform Domain Techniques

(i) Spatial Domain:
These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image.

(ii) Transform Domain:

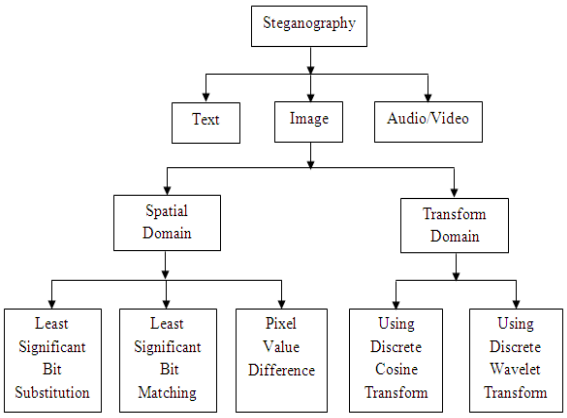


Fig: Various Steganography techniques

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in the transform domain is widely used for robust watermarking. Similar techniques can also realize largecapacity embedding for steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT).

2 .1 SPATIAL DOMAIN TECHNIQUES:

(i) Least Significant Bit (LSB):
The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) replacement technique in which the least significant bit of the binary representation of the pixel gray levels is used to represent the message bit.

(ii) Pixel Value Differencing (PVD):
A similar kind of algorithm based on human vision sensitivity has been proposed by the name of Pixel Value Differencing. This approach is based on adding more amounts of data bits in the high variance regions of the image for example near "the edges" by considering the difference values of two neighboring pixels. This approach has been improved further by clubbing it with least significant bit embedding in.

(iii) Edges based data embedding method (EBE):
Edge Detection algorithm hides secret data into the pixels that make up the extracted edges of the carrier image. The secret data can be of any type, not necessarily text, and they are actually concealed into the three LSBs (Least Significant Bits) of the pixels of the carrier image, but not in every pixel, only in the ones that are part of the edges detected by the edge detection algorithm.

(iv) Random pixel embedding method (RPE):
In this algorithm data is hidden randomly i.e., data is hidden in some randomly selected pixel. Random pixel is generated by using Fibonacci algorithm.

(v) Mapping pixel to hidden data method (PMM):
The method for information hiding within the spatial domain of an image. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbors lies at the boundary of the image or not. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel.

(vi) Labeling or connectivity method:
A morphological processing starts at the peaks in the marker image and spreads throughout the rest of the image based on the connectivity of the pixels. Connectivity defines which pixels are connected to other pixels. A group of pixels that connected based on Connectivity types called an Object.

(vii) Pixel intensity or gray level value (GLV) based method:
Technique which is used to map data by modifying the gray level of the image pixels. Modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels.

This technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

(viii) Text based method:
In this technique the secret and host images are divided into blocks of specific size and each block in secret image is taken as a texture pattern for which the most similar block is found among the blocks of the host image. The embedding procedure is carried on by replacing these small blocks of the secret image with blocks in host image in such a way that least distortion would be imposed on it.

(ix) Histogram based method:
In histogram based data hiding technique the crucial information is embedded into the image histogram. Pairs of peak points and zero points are used to achieve low embedding distortion with respect to providing low data hiding capacity.

(x) Spread Spectrum based methods:
The core of spread spectrum image steganography (SSIS) is a spread spectrum encoder. These devices work by modulating a narrow band signal over a carrier. The carrier's frequency is continually shifted using a pseudorandom noise generator feeded with a secret key. In this way the spectral energy of the signal is spread over a wide band, thus decreasing its density, usually under the noise level. To extract the embedded message, the receiver must use the same key and noise generator to tune on the right frequencies and demodulate the original signal. A casual observer won't be able even to detect the hidden communication, since it is under the noise level.

(xi) Color Palette based methods:
The palette based image steganography is similar to the commonly used LSB method for 24 bit color images (or 8 bit grayscale images).
After the palette colors are sorted by luminance, it embeds the message into the LSB of indices pointing to the palette colors. Message recovery is simply achieved by selecting the same pixels and collecting the LSBs of all indices to the ordered palette.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

2.3 ADVANTAGES AND DISADVANTAGES OF SPATIAL DOMAIN TECHNIQUE:

General advantages of Spatial Domain Technique are-

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.
3. Low Mathematical Complexity.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.
3. The information may be segmented on a particular part of image.
4. Typically depend on the image format.

2.3.1 TRANSFORM DOMAIN TECHNIQUES:

Transform domain techniques are broadly classified into:

(A) DISCRETE COSINE TRANSFORM (DCT) BASED TECHNIQUE:

DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted.

(B) DISCRETE FOURIER TRANSFORM (DFT) BASED TECHNIQUE:

The DFT based technique is similar to the DCT based technique but it utilizes the Fourier transform instead of cosine which makes it lack resistance to strong geometric distortions. Although it increases the overall complexity of the process.

(C) DWT BASED:

A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. To analyze a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). This method transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object.

(D) IWT BASED:

Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters (and also the other filters like DCT, FFT) have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image.

(E) DCVT BASED:

Curvelet transform is the new member of the evolving family of multiscale geometric transforms. Since it represents edges better than Wavelet, Curvelet transform offers an effective solution to the problems associated with image steganography using Wavelets and DCT (Discrete Cosine Transform).

2.3.2 ADVANTAGES AND DISADVANTAGES OF TRANSFORM DOMAIN TECHNIQUE:

General advantages of transform domain technique are:

1. There is less chance for removal or loss of the hidden data.
2. Information is distributed over all whole image.
3. Provides much higher flexibility for hiding data.
4. Typically independent of the image format.

Disadvantages of transform technique are:

1. Greater understanding of the embedding domain required.
2. Careful selection of embedding coefficients required otherwise it can cause degradation of image.
3. Higher Mathematical Complexity.
4. Relatively Low embedding capacity.

2.3.3 HANDLING IMAGE DATA

The java.awt.image.BufferedImage class in Java provides a versatile set of functions for handling the most common types of images. It provides for getting and setting the value of each pixel and permits splitting the pixel value into its alpha, red, green and blue components.

Table 1 shows the most useful methods of the BufferedImage class for accessing pixel values.

Table 1 Useful Methods java.awt.image.BufferedImage class

Sl. No.	Method	Purpose
1.	getWidth()	Get the width of image in pixels.
2.	getHeight()	Get the height of image in pixels.
3.	getSubImage(int x, int y, int width, int height)	Get a portion of image within the rectangular space indicated by the x, y, width and height values.
4.	getRGB(int x, int y)	This method returns the Alpha, Red, Green and Blue values (ARGB) of a

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

		pixel packed in an integer. The first byte (bits 0 to 7) represent Alpha value, the second byte (bits 8 to 15) represent Red colour, third byte (bits 16 to 23) represent Green and the last byte (bits 24 to 31) represent Blue colour.
5.	setRGB(int x, int y, intpixel)	Embeds given pixel value at location x, y.

For reading image files and writing them back into disk, the read and write methods of the class javax.imageio.ImageIO are useful. After getting the pixel value, we have to embed desired information into the image file in by accessing the appropriate bits and setting their values.

3. IMAGE FORMATS SUITABLE FOR EMBEDDING MESSAGES

Most of the image formats store image data in some form of compression. The compression algorithms used for image data can be divided into two broad categories: i) lossy compression algorithms (JPG, GIFF etc.) and ii) loss-less compression algorithms (PNG, BMP, DEB, etc.). Lossy compression algorithms result in significantly small file size. But, the actual value of each pixel of the original image is not preserved. i.e., the algorithm achieves very high compression level and very small file size by sacrificing the exact value of each pixel and subjecting pixel values to some form of grouping. Lossy compression is not suitable for steganographic transmission of messages, since the pixel values may be modified by the algorithm after we embed the message.

In loss-less compression, the algorithm compresses the image, but does not make any changes to the value of each pixel of the original image. The loss-less compression algorithm is suitable for storing steganographic messages. The pixel values of the new image are the exact replica of the original image except for the bits we modified for embedding our message.

In the present case, the image containing required message should be saved in loss-less compression formats like PNG, BMP, DEB etc.

3.1 FORMAT OF IMAGE DATA

Images are constructed using tiny dots named pixels. Each pixel has got its own attributes for displaying colour and transparency. There are several systems available for representing colour in image pixel. The most common system for representing colour is the ARGB system – which stores pixel data in the form of red, green, blue and alpha (transparency). The code shown in this article uses ARGB system for storing and manipulating pixel data.

Under ARGB system, first 8 bits (0 to 7) of the pixel belong to Alpha value or the transparency value. The second 8 bits (8 to 15) represent red colour, third 8 bits (16 to 23) represent green colour and the last 8 bits (24 to 31) represent blue colour.

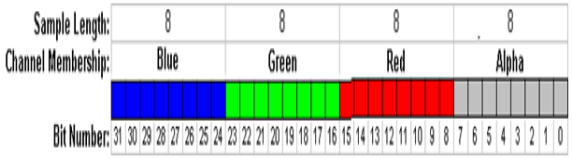


Fig.1 Organization of a Pixel under ARGB System

Now that the pixel level organization of ARGB system is clear, we should understand that that the maximum value for each parameter of ARGB system is 28 , i.e., 256. Maximum value is shown when the pixel stores one in all bits. If a change is made to the value at the least significant bit, i.e. the bit location 0 for alpha value, 8 for red value, 16 for green value and 24 for blue value, the impact is likely to be 0.39% $\left(\frac{1}{256} x100 \right)$. Since the change in original value is very low, we might use the least significant bit of any or all the four ARGB bytes for storing the information we wish to transmit incognito.

3.2 STRATEGY FOR STORING MESSAGE IN AN IMAGE

The present example uses only the least significant bit of the alpha part of a pixel. This example does not modify any colour value. Before embedding the message, the length of the message should be written into the image. This will exclude the appearance of junk values in the decoded message.

After extracting bit number 0 from the first 32 pixels, the bits should be neatly arranged inside an integer variable to know the length of message embedded into the image. Pixels following the 32nd pixel store the bits needed for reconstructing the byte value needed to create the original string.

Hence, an image with 1 million pixels (or 1 Mega Pixel) might be able to store a message containing a maximum of 1,24,996 characters. ((1,000,000-32)/8 = 1,24,996). Although 1 Mega Pixel image is considered a low resolution image, it could store a lot of characters in the form of a text message. Maximum size of message that could be embedded in an image at the rate of 1 bit from each pixel can be calculated using the relation $n = \frac{(P-32)}{8}$. If we increase the storage locations for message to the least significant bit of all the four components of ARGB system (pixel numbers 0, 8, 16 and 24), the storage capacity increases to $n = \frac{(4P-8)}{8}$.

Here, n is the maximum length of message and P is the number of pixels.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Since we have gathered sufficient information on the procedure for storing message inside an image, it is time we implemented the procedure**.**

Proposed system:

The basic ideas of the proposed data hiding scheme are:

(i) To use a different binary operator XOR to protect the secret key from being compromised.

(ii) To use a weight matrix to increase the data hiding rate while maintaining high quality of the host image.

$$F_i = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} K = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} W = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

$$F_i \oplus K = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

The inputs to our scheme are:

- F: a host Bitmap, which is to be modified to embed data.
- K: a secret key shared by the sender and the receiver. It is randomly selected bitmap of size m×n.
- W: a secret weight matrix shared by the sender and receiver.
- r: the number of bits to be embedded in each m×n block of F.
- B: some critical information consisting of kr bits to be embedded in F, where k is the number of m×n blocks in F.

$$(F_i \oplus K) \otimes W = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{bmatrix}$$

$F =$

F_1				F_2			
0	1	0	1	0	1	1	0
1	0	0	0	1	1	1	1
1	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0
1	1	1	0	1	0	0	0
0	0	1	1	1	0	1	0
1	1	0	1	0	1	1	1
1	0	1	1	0	1	1	1
F_3				F_4			

$K =$

1	1	0	0
0	1	0	0
1	1	1	0
0	0	1	0

$W =$

1	2	3	4
5	6	7	1
2	3	4	5
6	7	1	2

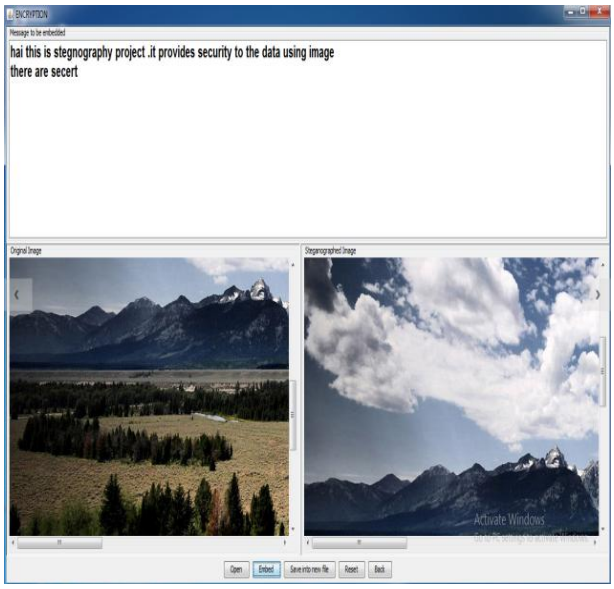
Fig. 3. An example of host image F, secret key K, and weight matrix W.

$F_1 \oplus K$				$F_2 \oplus K$			
1	0	0	1	1	0	1	0
1	1	0	0	1	0	1	1
0	1	1	0	1	1	1	0
0	0	1	0	0	0	0	1
0	0	1	0	0	1	0	0
0	1	1	1	1	1	1	0
0	0	1	1	1	0	0	1
1	0	0	1	0	1	0	1
$F_3 \oplus K$				$F_4 \oplus K$			

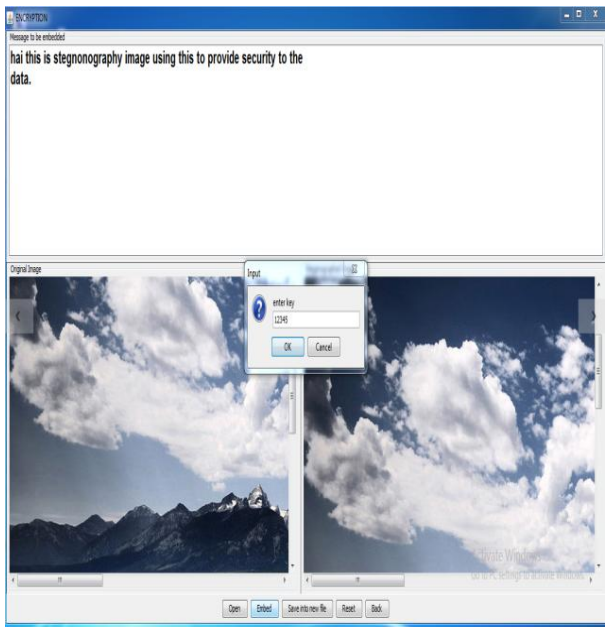
F_1'				F_2'			
0	1	0	1	0	1	1	0
1	0	0	1	1	1	1	1
1	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0
1	1	1	0	1	0	0	0
0	0	1	1	1	1	1	0
1	1	0	1	0	0	1	1
1	0	1	0	0	1	1	1
F_3'				F_4'			

Fig. 4. (a) $F \oplus K$, and (b) the modified host image.

Encryption Image1:



Encryption Image2



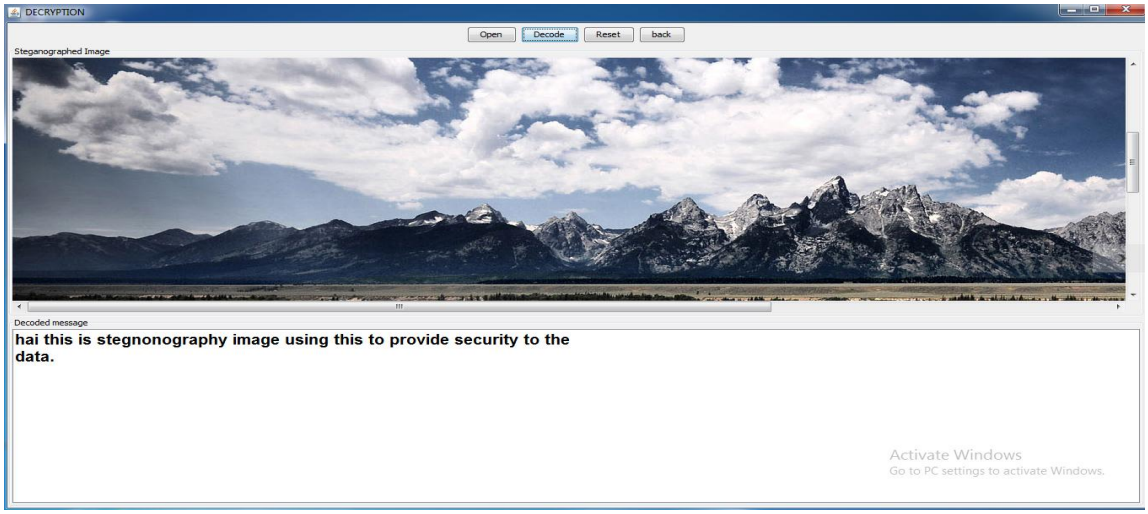
DOI 10.17148/IJARCCE.2016.5845

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

DECRYPTION IMAGE:



4. CONCLUSION

We have studied how to hide a piece of critical information in a host binary image using the concept of steganography. The main idea is how to use the secret key to protect the hidden data. Analysis and experiments both show that our scheme is more secure and more efficient, than an existing scheme. As to future research. we are currently investigating approaches to reduce the visibility of noises in the host image after data embedding.

REFERENCES

[1] M.Y.Wu and J.H.Lee. A Novel Data Embedding Method for Two-Color Facsimile Images.
[2] W. Stallings. Cryptography and Network Security.
[3] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne. A Digital Watermark.
[4] R.J. Anderson. Stretching the Limits of Steganography.
[5] 5.https://www.google.co.in/?gfe_rd=cr&ei=UqAVrafFqTv8wfYsLuACQ&gws _rd=ssl#q=image+steganography
[6] Introduction to Steganography.
[7] An Over-View of image steganography by Martin S Olivier.