National Conference on Engineering, Science, Technology in Industrial Application and Significance of Free Open Source Softwares Organized by K G REDDY College of Engineering & Technology & IJCRT.ORG 2017

Information Secured Steelth Steganography Using MMS (SSS in MMS)

[1]N.V.L.Neelima[1], [2]D.Himabindu[2], [3]Rambabu M

1B.Tech, Student, Department of Computer Science and Engineering, KG Reddy College of Engineering and Technology, Hyderabad,,Email:neelimaneeluaug@gmail.com

2B.Tech, Student, Department of Computer Science and Engineering, KG Reddy college of Engineering and Technology,Hyderabad, Email:dbindu521@gmail.com

3M.Tech, Associate professor, Department of Computer Science and Engineering G Reddy College of Engineering and Technology, Hyderabad,

Abstract: Steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography is the word derived from Greek. Stego means hiding, graphy means writing. It is the science of embedding information into the cover image viz., text, video and image without causing statistically significant modification to the cover image. If the selected image is color image, then convert the image into pixels and the pixels into cells. Read each pixel and generate the color code for that pixel. Here we use LSB(least significant bit) technique to hide the message into the image. LSB data hiding technique does not affect the visible properties of the image. For using LSB technique, we first convert the color code into binary language. Now by using LSB technique, we change the least significant bit value for the binary code generated before. So after changing the least significant bit value whatever value we get, for that number we see the color code and then we hide our text in that pixel which will contain that particular color code. Repeat this process until we hide our full message.

Keywords: - Steganography, Cover image, Pixels, Cells, LSBTechnique, Binary code.

1. INTRODUCTION

The communication security remains as a serious concern in information security. Secure data transfer is the need of every time. A number of hardware and software solutions have been proposed and implemented for information security, which restrict the unauthorized access, disclosure and malicious use of personal and classified information etc. Data hiding is a popularly used technique for secure communication. Data hiding is the technique of embedding information into digital content without causing perceptual degradation. Watermarking, cryptography and steganography are three famous techniques used in data hiding.

Cryptography is a popularly used technique for secure communication in the presence of third parties. Cryptography was synonymous with encryption, which involve the conversion of information from a readable form to apparent nonsense. A particular decoding technique will be required to decrypt or recover the original information from an encrypted message. The source of an encrypted message shares the decoding technique only with intendedrecipients; thereby avoid the unauthorized or unintended third party access to the secret information.

Steganography is considered to be the art of hiding information. In steganography the existence of the message itself is not disguised, but the content is obscure. The goal of steganography is to hide information such that the adversary is completely unaware of the communication. Steganography focuses on keeping the existence of hidden information undetectable to human eyes. Steganography involves any process that deals with hiding data or information within another data. The main motive of steganography technique is to prevent detection of hidden information and thereby ensure secure information transfer. In Greek steganography is defined as covering writing. Majority of the steganography techniques have been developed and computerized steganography usage have been started only by 2000. Batch steganography, permutation steganography, least significant bit(LSB), bit plane complexity segmentation(BPCS) and chaos based spread spectrum image steganography(CSSIS) are some of the steganography techniques used for data hiding. In this paper, we use the LSB Technique to hide the secret message within the cover image.

One of the common and simple approach for image steganography is the least significant bit (LSB) insertion method. This LSB based technique can be used to hide an image within another image. This involves replacement of LSB's of cover image pixels with secret image bits. Thus an image is hidden inside another image by altering only the LSB's of the cover. The change in LSB does not make

much effect on the cover image and hence it will not give even an idea that some information is hidden behind the image. Several steganography techniques based on least significant bit insertion method have been proposed and implemented. When LSB insertion method is employed on a 24-bit image, three bits can be encoded into each pixel, since each pixel is represented by three bytes. Changes in these LSB bits will be imperceptible to the human eye. When LSB techniques are employed on 8-bit color images, more care need to be taken. So, when 8 bit images are used as cover the greyimages are recommended for data hiding.

2. LITERATURE SURVEY

Image is represented with various light intensities, which is represented by pixels of the image and pixels represent a number. So image is an array of pixel values having different values at different locations.

Digital images typically have either 24-bit or 8-bit representation. ie. either 24 bits or 8 bits are used to represent a pixel. 24-bit images are the true color images and they offer more space for hiding information. However, 24-bit images are generally large in size and not that common, and they would attract attention when they are transmitted across a network or the Internet. So generally 8 bits images like GIF files are used to hide information, in which each pixel is represented by a single byte. So each pixel can have values ranges from 0 to 255 and which in turn represent 256 colors.

Least Significant Bit (LSB) insertion method is a common and simple approach for image steganography. This technique allows hiding information within an image by replacing the LSB's of the cover image. Replacement of LSB does not make changes on the cover image and henceintended user will not get the idea of secret information. The existing method of image steganography using plain LSB insertion method replaces only the least significant bit of each of the pixel of the cover image. i.e. only a single bit is replaced in each pixel. The LSB replacement allows hiding information behind cover image directly. And since it change only a single bit of a pixel it do not cause detectable difference in image quality.

The Four bit and Six bit data hiding methods which are based on LSB steganography can be used to improve the information carrying capacity of cover image used. In plain LSB method since a single LSB bit is modified in each pixel and each pixel is represented with 8 bits, the cover image is required to be 8 times bigger than the secret image. The 4 bit and 6 bit methods modifies more number of LSB bits and thus the size requirement of cover image in plain LSB method is reduced by these methods.

In 4 bit data hiding method the last four LSB bits of each of the cover image pixel is replaced with corresponding first four MSB bits of secret image. ie. This method embeds the 4 MSB bits of secret image into 4 LSB bits of cover image. The 6 bit method embeds 6 MSB bits of each pixel of secret image into LSB bits of two cover image pixels, 3 bits on each pixel. ie. 3 LSB bits of cover image pixels will be modified. Thus six bit data hiding method embeds first 3 MSB bits of secret image to last 3 LSB bits of a cover image pixel. Again the next 3 bits of secret image is placed in 3 LSB bits of next pixel of cover image.

3. **Proposed System**

The paper proposes the steganographic technique of 3 bit data hiding method which is based on LSB steganography. In the existing plain LSB approach the large size requirement of cover image remain as a disadvantage. ie. The cover image is required to be at least 8 times bigger than the message image. The 4 bit and 6 bit LSB data hiding methods overcome this size requirement. But quality of retrieved image is not offered by these methods. Another big disadvantage of these methods is the sequence-mapping problem. i.e. There is a direct mapping between cover image and secret image pixels. Due to this simplicity of these methods an attacker who suspects that some formation is hidden behind the cover image, he can easily extract information by just collecting LSBs of stego image. The proposed method of 3 bit LSB steganography is a solution to these problems.

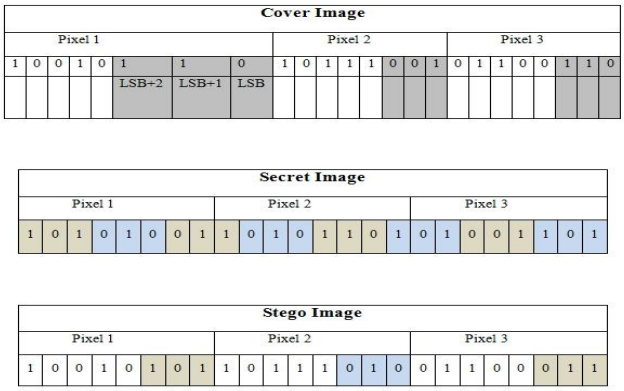


Figure 1: 3 bit data hiding method

In 3 bit data hiding technique the secret image bits are taken 3 at a time. Each of the 3 bits of secret image is embedded into last 3 LSB bits of cover image pixels. So last 3 bits cover image pixels are replaced with secret image bits. Thus with each of the 8 bits the cover image pixel 3 bit will be secret information. The Figure 1 shows the 3 bit data hiding method. Since all the secret image bits are embedded in the cover image, secret image can be retrieved from cover image with exact quality by this method. This 3 bit data hiding technique avoid the sequence mapping problem and enhances the LSB technique by incorporating randomization with LSB insertion. By this the secret image bits will be randomly dispersed in the cover image pixels and thus makeit harder for unauthorized people to extract the hidden image.

LSB steganography with randomization:

The existing LSB techniques are considered easy and direct methods to hide an image in a cover image. The information is embedded using the concept of sequence-mapping. Even though LSB technique hides the information in such way that the humans do not recognize its existence, still there exists the possibility of retrieving the secret information due to the simplicity of the technique

Therefore, we propose the randomization technique to improve the security of LSB scheme. This method embeds the secret image bits into random pixels of the cover image. And thus this allows overcoming the sequence mapping problem and making the system more secure. The RC4 algorithm is used for implementing this randomization. The RC4 algorithm generates the pixels of cover image in a random order and the secret image bits are embedded into these pixels in the respective order. Since RC4 have very simple structure and can be implemented efficiently RC4 is widely used. RC4 also offers simple key scheduling and output generation process. Since the secret information is randomly dispersed it is more difficult for an intruder to extract the hidden information. This algorithm makes use of a stego-key which is required during embedding and extracting the secret information. This stego-key can be made available at the receiver by embedding within the transmitting image or can be supplied to the receiver separately. In the absence of stego-key it is very hard to know the sequence in which cover image pixels are used for embedding the information. Thus this RC4 based randomization improves the security of the system.

Following steps describes how RC4 algorithm is used to generate random cover image pixels.

Step 1: Pixilate both the images

Step 2: Generate array of cover image locations for selected stego-key using RC4 algorithm.

Step 3: Replace the LSBs of cover image pixels in the sequence generated in step 2, with message image bits

Thus the proposed method offers improvement in information carrying capacity with improved security and quality.

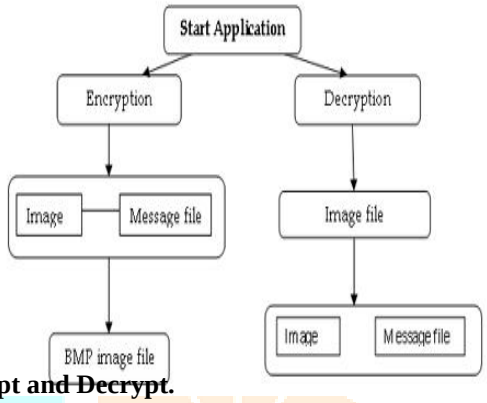
OBJECTIVES:

- To understand a new methodology of LSB technique in order to gain quality of the picture
- To achieve the security that is not possible through 4-bit and 6-bit

- Using RC4, we achieve randomization which will make difficult for any intruder to find the hidden information
- Also there is no requirement of taking a bigger size cover image to hide the image.

4.IMPLEMENTATION

Graphical Representation. The graphical representation of Steganography system is as follows:



The two methods are – Encrypt and Decrypt.

In encryption the secret information is hiding in with any type of image file.Decryption is getting the secret information from image file.

ENCRYPTION PROCESS:

INFORMATION FILE BMP FILE

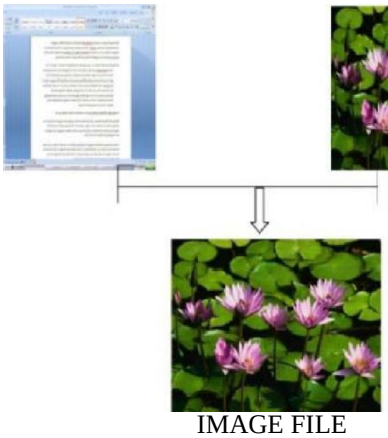
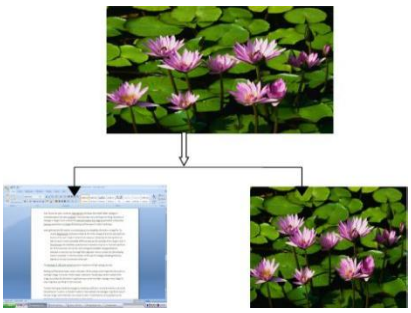


IMAGE FILE

DECRYPTION PROCESS:

BMP FILE



INFORMATION FILE IMAGE FILE

RC4 Algorithm

The proposed method consist of these steps

1.Consider a cover video.

2.first convert Video into frames.

3.encrypt a message using RC4 Cryptographic algorithm.

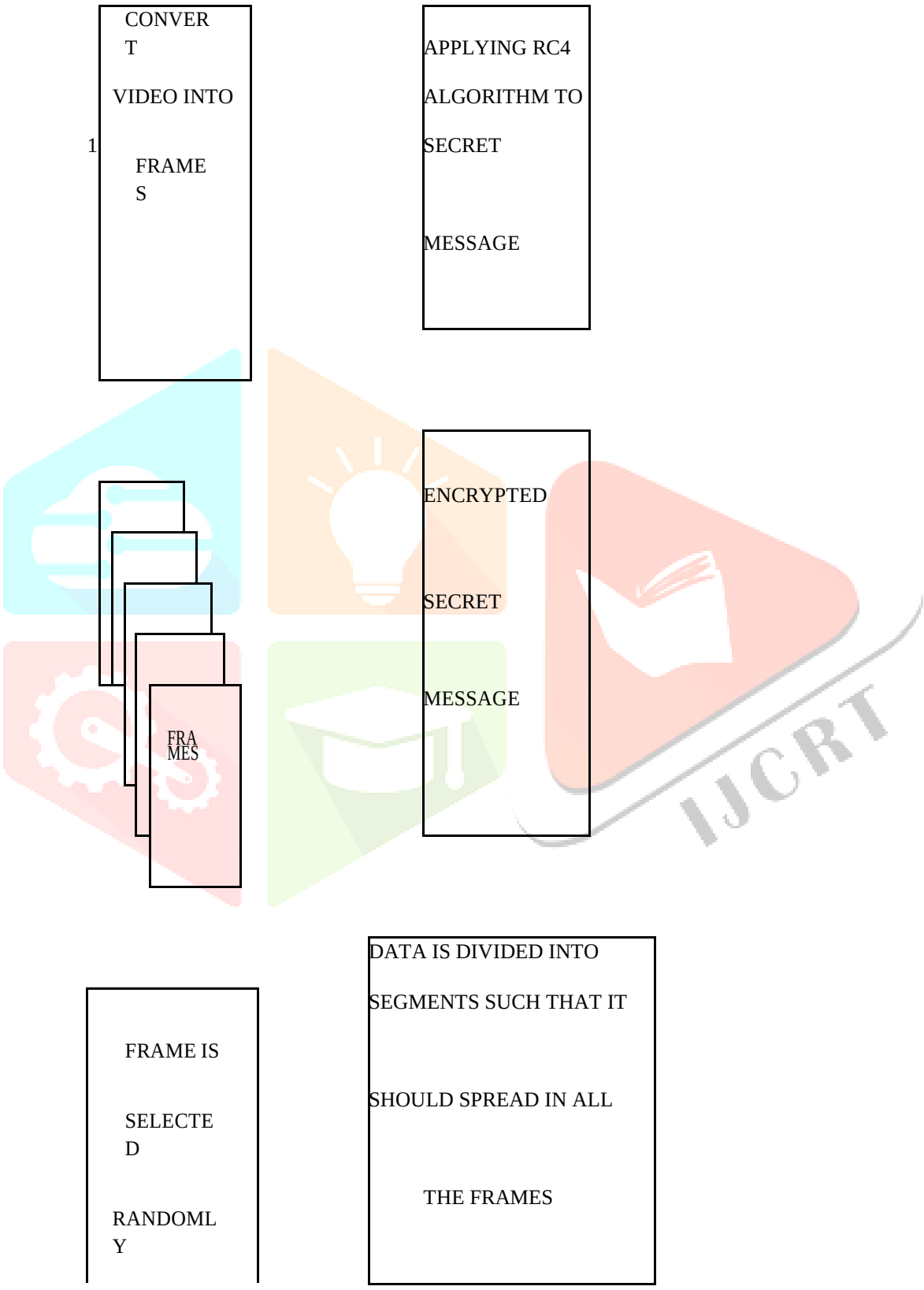
4.Frames are randomly selected.

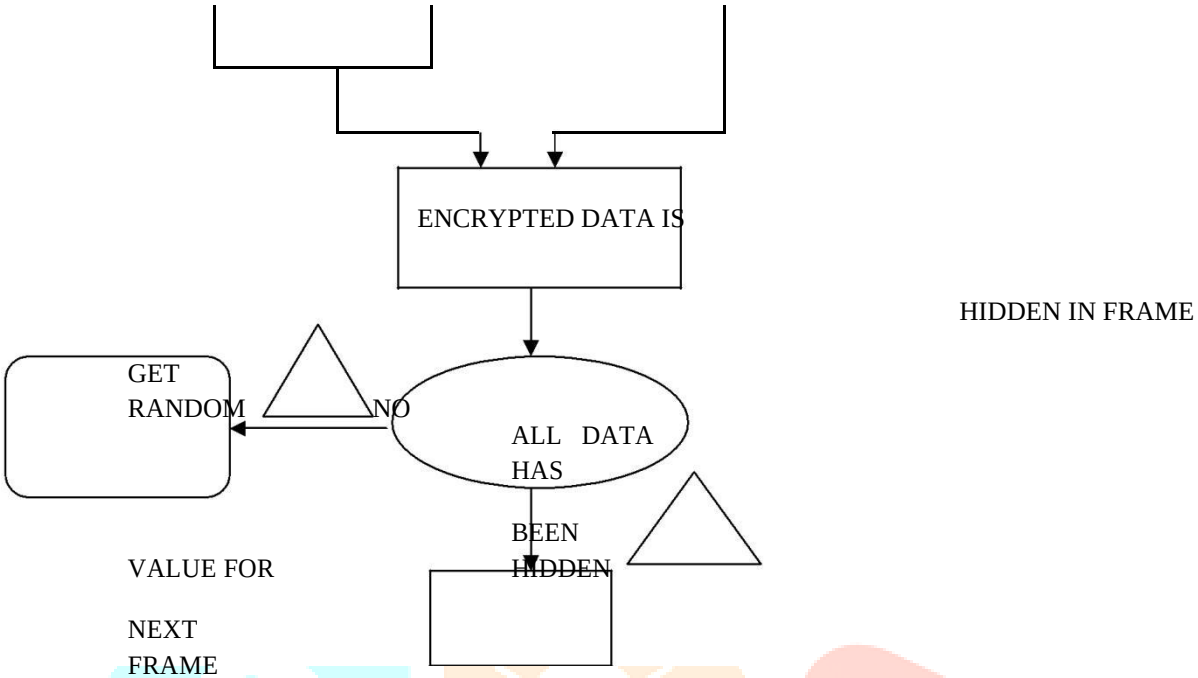
5.embed the encrypted message inside a video frames.

The aim of the proposed approach to embed the secret message in video frames of the cover video. In this approach we first convert Video into frames and then encrypt a message using RC4 Cryptographic algorithm to enhance the secrecy of the message and then embed the encrypted message inside a video frames. For insertion of message in frames, frames are selected in random manner. In this way secret message is embedded in random manners in frames and frame is selected randomly until all message is hidden. Our research focuses on providing a solution for transferring and sharing important data without any compromise in security.

COVER VIDEO

SECRET MESSAGE


CONVERT
VIDEO INTO
1
FRAMES
APPLYING RC4
ALGORITHM TO
SECRET
MESSAGE
ENCRYPTED
SECRET
MESSAGE
FRAMES
FRAME IS
SELECTED
RANDOMLY
DATA IS DIVIDED INTO
SEGMENTS SUCH THAT IT
SHOULD SPREAD IN ALL
THE FRAMES

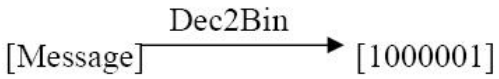


Least Significant Bit (LSB)

In Steganography, The most well known techniques to data hiding in images are least significant bit (LSB) substitution, and masking & filtering techniques. LSB is a simple approach to embedding information in an image. But image manipulation can destroy the hidden information in this image. Applying LSB technique to each byte of a 24-bit image,three bits can be encoded into each pixel, as each pixel is represented by three bytes. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte.

Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganography methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacingsome of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates (12). The following steps illustrate how this method is used to hide the secret data "A" in cover image "Mansoura.bmp" (12).

Step1: Convert the data from decimal to binary.



Step2: Read Cover Image "Mansoura.bmp" as shown in Fig3,

144	142	146	152	156	147	151	157
160	155	159	162	133	123	133	145
144	141	141	138	61	55	65	79
120	123	131	144	50	61	74	92
170	167	167	166	61	59	56	59
120	125	131	132	61	59	59	59
124	133	139	131	88	76	77	76
138	153	167	154	139	.....	.....	.....

Fig 17.3 The cover image “Mansoura.bmp"

Step3: Convert the Cover Image from decimal to binary.

10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101
10100000	10011011	10011111	10100010	10000101	01111011	10000101	10010001
10010000	10001101	10001101	10001010	00111101	00110111	01000001	01001111
01111000	01111011	10000011	10010000	00110010	00111101	01001010	01011100
10101010	10100111	10100111	10100110	00111101	00111011	00111000	00111011
01111000	01111101	10000011	10000100	00111101	00111011	00111011	00111011
01111100	10000101	10000111	10000011	01011000	01001100	01001101	01001100
10001010	10011001	10100111	10011010	10001011	.....	.....	.....

Step4: Break the byte to be hidden into bits.

Thus [10000001]is divided into 8 bits [1 0 0 0 0 0 0 1].

Step5: Take first 8 byte of original data from the Cover Image.

10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101

Step6: Replace the least significant bit by one bit of the data to be hidden as follows,First byte of original data from the Cover Image

A simplified example with a 24-bit image

1 pixel:

(00100111 11101001 11001000)

Insert 101:

(00100111 11101000 11001001)

red green blue

Repeat the replace for all bytes of cover image.

Finally the cover image before and after steganography is shown in the following figure.

Cover image before steganography

Cover image after steganography

Conclusion

Steganography is an efficient technique that can be used for secret information transfer. This technique allows hiding an image, which is a secret, into a cover image. Steganography provides an effective way of secret communication since the attacker is unable to detect the presence of hidden secret information. The least significant bit (LSB) based steganography is a common and simple approach for embedding information in images. We present a LSB based steganography method which is more secure and strong than existing LSB method.

We propose an image hiding technique which allows hiding an image within another image. The proposed method improves the security of normal LSB based steganography. And also improve the information carrying capacity of cover image compared to plain LSB. The system make use of LSB(Least Significant Bit) based image steganography and the proposed 3 bit data hiding method improve the quality of secret image retrieved at the receiver.

For security enhancement, the order of selected cover-image pixel for embedding the secret image bits depends on the random numbers generated by the RC4 using a shared key. Even if an attacker identifies the existence of hidden information in a cover, it is difficult for him to recover it because the bits are embedded in a random order. The 3 bit data hiding method hides all the secret image bits at the same time offers improvement in information carrying capacity and allows regenerating the secret image at exact quality at the receiver.

The security of the proposed system can be further improved by incorporating cryptographic encryption with the system. The secret image which is to be hidden can be encrypted before performing the proposed LSB technique. This could be considered in future.

REFERENCES

- T. Morkel, J.H.P. Eloff, M.S. Olivier AN OVERVIEW OF IMAGE STEGANOGRAPHY, ,Information and Computer Security Architecture (ICSA) Research Group,Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa
- Moerland, T., “Steganography and Steganalysis”, *Leiden Institute ofAdvanced Computing Science*,www.liacs.nl/home/tmoerl/privtech.pdf
- Silman, J., “Steganography and Steganalysis: An Overview”, *SANSInstitute*, 2001

- Jamil, T., "Steganography: The art of hiding information is plain sight",*IEEE Potentials*, 18:01, 1999
- Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*,47:10, October 2004
- Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography",*IEEE Journal of selected Areas in Communications*, May 1998
- Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactions on image processing, 8:08,* 1999
- Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002