An improved LSB based Steganography with enhanced Security and Embedding/Extraction

Mamta Juneja and Parvinder S. Sandhu

Abstract—The proposed system is an approach used to embed text into gray image (BMP). It enables the user to provide the system with both text and cover, and obtain a resulting image that contains the hidden text inside. The system uses the least significant Bit (LSB) method to embed the secret text in image after encrypt the secret text using RC4 stream cipher method and store the text in non sequential pixel in image by using variable hope value power of 2[2, 4, 8, 16, 32]. The Proposed system aim to provide improved robustness, security due to multi-level security architecture along with faster embedding and extraction process irrespective of size of embedded text.

Keywords—Steganography, RC4 stream cipher method, LSB technique.

I. INTRODUCTION

STEGANOGRAPHY is the art and science of writing hidden messages in such a way that no one except from the intended recipient knows of the existence of the message. Steganography literally means “covered message” and involves transmitting secret messages through seemingly innocuous files. In terms of “Digital steganography”, a file can be hidden inside another file. Current digital techniques do not tend to take the cover (where the message is hidden) into account, and thus leaving marks on the stego-object (what the object becomes after hiding information). To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in “noisy” areas that draw less attention those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

• Least significant bit insertion
• Masking and filtering
• Redundant Pattern Encoding
• Encrypt and Scatter
• Algorithms and transformations.

Each of these techniques can be applied, with varying degrees of success but the one which is implemented in our proposed system is Least significant bit insertion.

1.1 Least significant bit insertion

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M’s bit. This technique works well for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object [1, 3].

1.2 RC4 (RANDOM BYTE GENERATION)

RC4 is the most widely used stream cipher in these days, especially for the software applications. This is because the structure of RC4 is very simple and can be implementing in software efficiently. Although RC4 has a huge internal state, it has the light-weight key scheduling and the output generation processes. It was seemed as a safe cryptography algorithm until 1994. In September, 1994, the algorithm was posted by someone on the Internet and is available for public analysis now [28].

RC4 Stream Cipher [28]

There are so many stream ciphers in these days, and most of them are implemented by using linear feedback shift registers. These stream ciphers are easy to implement in hardware but may not be in the software. In 1987, Ron Rivest developed the RC4 stream cipher. It is suitable for software applications, and is used widely nowadays. For example, RC4 is used in SSL (Secure Sockets Layer) protocol. It is also be used in WEP (Wired Equivalent Privacy) and many network applications.

The algorithm of RC4 can be seen to have 4 stages. The essential parts of this cipher are:

• A simple basic counter, modulo the table size.
• Another pointer that is updated using a table value
• Output a value that depends on table value of both pointers
• Update the table

II. DESIGN OF PROPOSES SYSTEM

The proposed system takes as an input the embedded – object which in our case a file of text (ASCII characters) and the cover-object which is a gray-scale image of size (256*256) pixels and produces on output stego-object which is a resulting image.

The proposed system stands for two main stages these are:-

1. Embedding secret text in the still image by using one (LSB Technique) from many proposed techniques of steganography hiding.
2. Extracting the stego text from many stego-object (image) when image received to other side. The figure 1 represents general block diagram of the proposed system.

**2.1 Embedding stage**

Embedding is the process of hiding the embedded message generating the stego image. Hiding information may require a Stegokey which is additional secret information, such as password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is stego image (stego object).

The main algorithm for the Embedded stage can be listed as follow:

1. Input the secret text (message) that to be hide in the cover image.
2. Select the cover image (BMP file) from list of image with size 256*256.
3. Open the cover image and read the data in matrix.
4. Select the value of variable hope power of 2 from available choices list [2, 4, 8, 12, 16, 24, and 32] for not sequentially embed the secret message.
5. Calculate the size of the secret text.
6. Apply RC4 stream cipher on secret text.
7. Substitute the encrypted secret characters of the text in the specified location (hope value) of the cover image.

The Block diagram of the encoder is shown in figure 2, the encoder consist of two stages, the first stage is the RC4 stream cipher which encrypt each byte of the secret text prior to the embedding process, the initial key of this operation is a random permutation of the numbers between 0 and 256. The second stage of the encoder is the LSB insertion mechanism, randomization of insertion the secret message bits into the image is verified by the employing of the offset, by this mechanism embed each bit from the ciphered secret text into 8-pixels from the cover image, the key of this operation is the number of offset or hopes employed to not sequentially embed each byte from ciphered secret text into 8-pixels from the cover image, the key of this operation is the number of offset or hopes employed to not sequentially embed each byte from ciphered secret text into the cover image the offset suggested by the package is the power of 2 (2, 4, 8, 16...).

For example suppose that the offset is "4", then the program will insert the first bit in byte 1, the second bit in byte 5, the third in byte 9 and so on. After reaching certain end, loop back starting from byte 2 then 6, 10, ... and so on.

**Figure 3 shows the flowchart of procedure RC4 stream cipher in details as explain in section (3-5-6)**
Select a value of variable “hope” from the available choices list [2, 4, 8, 12, 16, 24, 32].

If (text_size < cover_image_size * 8 + 16)

Yes

No

GO to RC4 function to generate random key

For f=0 to count

\[ P_{MESSAGE}_{ciphertext}[f] = (key[f]) \text{XOR} (P_{MESSAGE1}[f]); \]

f=f+1

Enter Embedding process

For i=0 to (count+2)

For a=0 to 8

a=a+1

i=i+1

Count1=0

For k=0 to hope

For i=0 to width_cover

For j=k to depth_cover

Count1=Count1+1

If Count1<Embedding_size

Write pixel of cover in stego_image without modification

Start LSBs with hope

Yes

No

Write setego image matrix in stego image file

End

2.2 Extracting stage

Extracting is the process of getting the embedded message out of the stego object again. New terminology with respect to attaches and breaking steganography schemes is similar to cryptographic terminology; however there are some significant differences. Just as a cryptanalyst applies Cryptanalysis in an attempt to decoder or crotch encrypted message, the stegonalyst is one who applies steganalysis in an attempt to detect the existence of hidden information.

After the stego object then is created and transmitted through a communication channel, if we assume ideal channel the stego object is received properly by the decoder circuit, again the decoder has two inputs (the extraction key and the stego object) and single output which is the secret text. The sequence of operation here is reversed, the LSB from stego object is first done then the ciphered secret text byte is gained, after that the final stage of RC4 decryption is done, the block diagram of this operation is illustrated in the figure 5.

The flow chart of extracting stage is shown in Fig 6 which describes the process in details.

III. IMPLEMENTATION OF PROPOSED SYSTEM

The simulation package for our system starts asking the user to select one from two phases: the first phase is writing in which the secret image is fed to the hiding software and the hiding process is begin Transferred to the second stage. Figure 7 illustrate first stage of the proposed package:
Stego_Extraction

Open the file of stego_image

Read the data matrix of stego image

pxl_Rcov [XD][YD]

Go to RC4 to generate the symmetric key for stream cipher

Extract hopes number from the cover image matrix pxl_Rcov

Count=0

Extract the length of text embedded in stego-image (len_txt)

i=0

Decipher vector of ciphered secret text data[len_txt] to get the secret text vector data[len_txt]

using the key generated by RC4

Count=Count+1

End routine

The package selects one of these images previously presented as shown in the figure 11 below.

The second stage of our proposed package starts by asking the user to select one of two actions: the first action is write, which is stands for writing secret message into the cover image, whereas the second action is to read the secret message from the cover image. When the first action is selected then the window in figure 8 is appeared in which the paragraph “writing secret TXT in image” is showed.

The third stage of the proposed algorithm includes the input of the secret message we want to embed inside the cover image. Figure 9 shows the details of this stage ,the text embedded is about 224 character.

The fourth stage of the proposed system involves the selection of the cover image from eight proposed image of gray scale with a size of (256*256) pixel, where each pixel is 8 bits , the proposed cover images are showed in figure 10

The second action implemented by this package is the reading operation. The reading process is aimed to read the...
secure text message embedded in the cover image selected by the writing stage. The first stage of reading process is started by asking about the password, like writing process. When we choose reading stage the window in figure 14 is appeared.

![Fig. 14 Window of Reading process](image)

The package in reading process display the secret key generated by the RC4 stream cipher generator, this algorithm generates random byte in each operation, then each byte is XORed with a character from the secret message to embed a ciphered message not the clear message in side the cover image. For our message proposed in figure (4.3) the key generated is illustrated in Fig 15:

![Fig.15 Window of RC4 key generation process](image)

Figure 16 displays the ciphered secret message which is embedded in the writing stage, of this package; all the ciphered characters are displayed in the ASCII character format.

![Fig. 16 Window Displays ciphered secret message](image)

The final stage in proposed algorithm is the extraction of the embedded secret text in its final and correct form. It is worth to mention that the code of the cover image with the size of the embedded text is also embedded in the cover image and the program when enter reading stage starts identifying these two item before it starts the operation of secret text extraction. Figure 17 displays the extracted secret message from the cover image with 100% accordance to the embedded text.

![Fig. 17 Window displays the extracted secret message from the cover image](image)

Figure 18 below gives the resulted stego-object for image called Lena, by applying proposed technique:

![Fig. 18 Stego-object for image called Lena](image)

The subjective quality between this image and the image presented in the figure 10 gives that the accordance between the two images is 100%.

### IV. SECURITY OF PROPOSED SYSTEM

The goal of Steganography is to avoid drawing suspicion to the transmission of hidden information, if suspicion is raised, then Steganography security is defected. On other hand the aim of cryptography is to convert intelligible information to unintelligible form, difficult for the third parties which not have a copy from the key. The proposed system achieves the union goal of security for the below reasons:

1. The results of proposed system stego-object is an image, this image is transmitted alone without the original image, this point enhance the security of system because there is little ability of matching between the original cover image and the stego-object.

2. The proposed system is build of multi-layer security, consequently even if the original copy of the stego-object is available, the intruder attacked by the second layer of security which is the encryption of the text embedded then he should analyze the cipher text using cipher text only attack which is difficult to be analyzed.

3. The password level of security is also added to our system, this layer of security should not be mixed with the two above layers, because it package oriented security layer, not security gained by algorithm presented, but it still effective and add more rigidity to the proposed system.

### V. CONCLUSION AND SUGGESTIONS FOR FUTURE WORK

The proposed system provides LSB method with RC4 stream cipher and hope for embedding text in image. A number of conclusions were derived from this study:

1. Steganography is not intended to replace cryptography but rather to supplement it. 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.

2. The proposed system can be defined as a secret key steganography since it shares a secret key between sender and receiver, in this system there is no need for the knowledge of original cover in the extraction process.

3. The amount of the information embedded in the other media depends on the statistical properties of the cover media, where this amount is small the noise in the media is not perceptible.

4. From the implementation we conclude that the proposed system is very rapid in performing extraction process and the size of the embedded text does not affect the speed of the system very much.
Many suggestions can be given to enhance the work of the proposed system they are:-

1. The method of embedding is trivial which is LSB insertion, in the future another embedding method should be employed like wavelet or DCT transform based methods.
2. Improved system to deals with video image and audio.
3. Using another file format of the images that are not used in our system such as JPEG, TIFF and GIF.
4. The Encryption method (RC4) could be replaced with RSA, or other public key ciphering algorithm to increase the security level.

REFERENCES