ABHIYANTRIKI

An International Journal of Engineering & Technology (A Peer Reviewed & Indexed Journal)

Vol. 3, No. 5 (May, 2016)

http://www.aijet.in/

eISSN: 2394-627X

Steganography using MATLAB

Srikant Pattnaik* Associate Professor GIET, Gunupur, Rayagada, Odisha, India Adarsh Kumar Dash UG Student GIET, Gunupur, Rayagada, Odisha, India

Asit Kumar Sahu UG Student GIET, Gunupur, Rayagada, Odisha, India

Abstract

Steganography is the process of concealing the identity of hidden message from the un-authorised parties other than intended receiver. This concealing nature is the advantage of steganography on cryptography because it attracts less attentions and messages passes with less suspicion. Steganography comes to picture where cryptography and other traditional encryption techniques outlaw. In this paper we are implementing steganography using two types of encoding namely sequential and random encoding using some functions in MATLAB environment. In this project user can manually select the cover image, type of encoding & type of message.

Keywords: MATLAB, Steganography, Sequential encoding, Random encoding.

*Author for correspondence srikantpatnaik@giet.edu

1. Introduction

In todays hustle and bustle world of Internet where users are actively participating in the web cyber space without having knowledge of the exposure on their private data and spaces. This involves the Internet which connects the whole world. This growth of the users and sharing of socialism has shifted its attention on one of the most important aspect of Internet. Since Internet is a public network, protecting the information on Internet is very important. Steganography has its unique place in security methods. It doesn't replace the encryption techniques but it supplements it. Steganography is on advantage as it reduces the chances of hidden message being detected and draws less suspicion unlike cryptography. Cryptography in turn disorders the messages whereas steganography hides the existence of message by making it invisible. Concept of "invisibility" hidden messages has increased the demand of steganography in many new fields than cryptography and digital watermarking techniques. It also produces better quality stego-images. There are two important components of the process the message and the carrier, message is the secret data to be transmitted and carrier is the cover to hide message.

2. Research Methodology

In this paper we are implementing two types of encoding. Let us see them briefly.

A. Sequential Encoding

This is the type of encoding where data is hidden in an image based on some fixed pattern that needs to be described. The same pattern should be included in the decoding process to get the hidden message. The pattern is the sequence of color channels of each pixel chosen to hide the data of grayscale converted "hide to image". A channel of each pixel is selected to replace the

grey value of that channel by the grey value of greyscale "hide to image". And the grey value of respective replaced channel will be stored for future decoding process.

Let the pattern be RGBBGRRGBBGR. Alternatively we are using RGB pattern and reversing it in the next attempt.

So here in this pattern we can say that the RED channel of first pixel will be used to hide the grey value of greyscale image (red channel grey value of first pixel will be replaced by grey value of hide to image). Similarly GREEN channel of second pixel and BLUE channel of third pixel will be used as before and the pattern will follow according to above mentioned. Sequential



encoding stores every message using this pattern is encoded from the Top Left pixel and is coded from Top to Bottom, Left to Right.

B. Random Encoding

Unlike sequential encoding this is considered to be more secure encoding method. It has a less probability of detection because it operates on a random sequence which is generated through the randperm function of MATLAB. More difficulty is to guessing the location of hidden message beacause of the input to randperm function is given through the user that is known as random seed. The random seed is only known to the sender and the intended receiver. Based on the input random seed the randperm function generates a permutation sequence on a random basis and that sequence is used to hide the data in the image by pixel count. The function stores random sequence generated for decoding purpose. Both the types of encoding uses



XOR operation for bit storage encoding and again XOR for decoding the bit. Random encoding holds the more secure encoding method than that of sequential encoding.

3. Research Analysis and Discussion

We are using some functions to operate the whole process of steganography. There exists a main steganography function which takes input from the user as cover image, type of encoding and the message (image or text). Based on type of encoding user needs to input different parameters. Then it controls the whole operation by calling the functions according to user choice. The functions are depicted below:

A. Steganography

This function provides a simple interface process that takes a user through the process of giving input based on user's choice.

Inputs / Outputs:

- No Inputs Required. User instead is prompted to provide necessary information.
- Automatically saves the cover image with encoded message as a Bitmap image or saves the decoded text or image message as a TXT or Bitmap file respectively.
- Returns encoded image or decoded message as a variable within MATLAB.

Features:

- User can select Encoding or Decoding and types.
- For Encoding process, the user needs to selects a cover carrier image to hide the message from a browsing prompt file window and then selects a text message or image file message from a browse file window. The program then prompts the user to decide upon an encoding method, encryption key and random seed before passing this information to the other functions. Then the function will return a Bitmap image as output that user needs to give the name of image file.
- For Decoding, the user needs to select the image containing the hidden message from a file window. The program then prompts the user to provide the encoding method, encryption key, and random seed before passing this information to the other functions for decoding. Then again the function will return the output as a new file named by user.

B. Stegancoder

Steganography function transfers control to this function if the encoding method is sequential. It receives the parameters from user and prepares header information by detecting the type of message (text or image). Then it encodes the message sequentially.

Inputs / Outputs:

- Requires a carrier image, text or image message, and encryption key as Inputs.
- Returns an image which has the message sequentially encoded as Output.

Features:

This function first determines the message type (text or image) and length and encodes this information as header information. Then the function sequentially encodes the message within the cover across the Red, Green, and Blue Channels of pixels in a specific pattern defined within the encoding function or as per choice of user he/she can design function accordingly. This means that every hide to message using this function is encoded from the Left most pixel and is

coded from up to down covering each single pixel, Left to Right. This is considered less secure than a Random Encoding.

C. Stegandecoder

This function complements the previous function in sequential encoding process. It is used in decoding of sequentially encoded messages. This file takes in the cover image and encryption key. It first decodes the header to determine the message type and message length, and then sequentially decodes and recovers the message.

Inputs / Outputs:

- Requires the sequentially encoded cover image and encryption key as Inputs.
- Returns the decoded text file or image file as an Output.

Features:

This function sequentially recovers the message values from the cover image by first separating the header information to determine message type and length. Then the function proceeds to decode the message using the length information from the header, and following the pattern that was used in the encoding process so by uses the encryption key to recover the values from RGB channels of pixels and decrypts the message.

D. Stegancoder_rand

Steganography function calls this function if the user choice is random encoding there by an extra user input called as random seed. This function determines the message type (text or image file), prepares header information to be used in the decoding stage, and randomly encodes the message within the pixel values (that is decided by the random seed) of the cover image.

Inputs / Outputs:

- Requires a cover image, text or image message, encryption key and random seed key as Inputs.
- Returns a bitmap image which has the message randomly encoded as Output.

Features:

This function first determines the message type and length and encodes this as header information (first 24 randomly encoded values). Then the function uses the randperm function to randomly select pixel locations to encode the message within. To do this the function determines the dimensions of the cover image , multiplies the dimensions together to provide the number of pixels available and uses randperm to randomly permutate a list from the resulted pixel value count available in a predictable and similar way by using the random seed key value given by user. This ensures that we don't overwrite message values in the cover image and can recover the message during the decoding stage. The function then uses the randperm list to encode the message values in the cover image. This function is faster.

E. Stegandecoder_rand

It is the complemented function of previous function as both implements random encoding process. This function is called if user needs to decode the message randomly. This file takes in the cover image, encryption key and random seed key. Firstly it decodes the header information

for message length and type. Then it decodes randomly by referring the precomputed list of randperm function.

Inputs / Outputs:

- Requires the encoded cover image, encryption key, and random seed key as Inputs.
- Returns the decoded text or image message as an Output.

Features:

This function uses the random seed key to initialize and recover the random pixel locations using the randperm function (inbuilt function of MATLAB for computing permutation list through a input provided). The function first calculates the dimension of cover image from stored 24

header bits and saved bits to determine the amount of pixels available before determining the permutated pixel locations using randperm. Next the function recovers randomly encoded message values from the cover image by first separating the header information to determine the message type and length. The function then proceeds to decode the rest of the message using the length information from the header, uses the encryption key to decrypt the message and returns the message.



4. Result

In encoded stage user will get prompts in command window of MATLAB as mentioned here. The above image depicts the procedure of steganography through which user has to provide inputs.

The whole process of steganography is explained in figure mentioned here.



Both the carrier image and stego image are alike that they look exactly the same by camouflaging the hidden message inside it.



5. Uses of Steganography

- Private data transfer in web space internet
- Banking systems and client service protection
- Intelligence and military service storage and message transmission

6. Future Scope

With increasing popularity of steganography many methods need to be implemented in order to make this technique more reliable, flexible and secure. It will provide a loss less secure transmission media for private and classified data without any suspicions of message transfer.

7. Conclusion

With taking the invisibility of hidden message it holds an advantage over other conventional encryption methods. Image steganography and its varieties are increasing in usage and many field applications. In areas where cryptography and strong encryption are being flawed, steganography provides such policies and pass messages covertly. As with the other great innovations of the digital age: the battle between information analysts, security experts and hackers, record companies and pirates, steganography continually evolve with new techniques to secure data.

References

- [1] Wikipedia
- [2] Google.com
- [3] Mathworks MATLAB