ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Image Steganography for Secure the Data using Least Significant Bit

Revathi. R.R[#1], Tamilarasi.P[*2], Vigneshwari.D[*3]

[1 2 3]*Dept. of Computer Applications, SA Engineering College, Chennai.*
revathishara@gmail.com, Tamilarasipavalan@gmail.com, vignesswari@gmail.com

Abstract— The rapid developed of data transfer through internet it make easy to send the accurate data and faster to the destination. For security purpose Image steganography is used with LSB (Least significant Bit) technique. Stenography is the art of hiding the information in some medium. The main idea of this paper is to secure the data during sending and receiving the file through internet and its disuse about a technique based on LSB algorithm with cryptography. Various techniques are used in Image steganography. RGB images used to secure the data in different channels. Image Steganography is shows how a text document to be hide in an image file.

Keywords—Least Significant Bit(LSB), carrier file, stego-key, Decryption, Encryption, Cryptography.

1. Introduction

The important factor of Information Technique and communication through Internet has been the security of information. Cryptography is the one of most famous techniques for secret communication. Various methods are available to develop encrypt and decrypt data to keep the message secret.

Steganography word is originated form Greek word. Stegano (Covered) and Graptos (Writing) Steganography means "Covered writing". Steganography is the branch of science it is used for writing hidden message in such a way that no one can able to read the message only the sender and receiver can read. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as steganalysis. The Purpose of both steganography and Cryptography is to provide secret communication.

Cryptography hides the contents of a secret message from an attacker, whereas steganography even cover up the existence of the message. Image Steganography is widely use for hiding process of data. Taking the cover object as image in Steganography is known as Image steganography.

It as terminologies are follows:

- Cover Image: For hiding the information the original image used as a carrier.
- Message: Actual information which is used to hide into images.
- Stego Images: After embedding message into cover images is known as stego images.
- Stego Key: A key is used for embedding the message from cover images and stego images.

2. Overview of Steganography

To provide an overview of steganography, terms and concepts should first be explained. An overview of the different kinds of steganography is given at a later stage.

2.1 Steganography Concept

Steganography is mostly used on the computers with digital data being the carriers and networks beings the highly speed delivery channels. The difference of steganography and cryptography is that the cryptography focuses on keeping the contents of a message secret whereas it's focuses on keeping the existence of secret. Steganography and cryptography both are ways for protecting information from unwanted parties using least significant bit technique. Two other technologies that are closely related to steganography are watermarking and fingerprinting.

A communication to contain hidden information, a passive administrator takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An *active* administrator, on the other side, will try to change the communication with the suspected hidden information intentionally, in order to remove the information.

2.2 Different kinds of Steganography

Secret message is hidden in various forms:

- Image.
- Audio.
- Video.
- Documents(Protocol).

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

3. Image Steganography

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric illustration forms a grid and the individual points are referred to as pixels. Most images on the world network comprise a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour. These pixels are presented horizontally row by row.

Bit depth is the number of bit in a colour schema, its related to the number of bits used for each pixel. The compression though, keeps the original digital image intact without the chance of lost, although is does not condense the image to such a small file size.

3.1 Image Compression

When working with larger images of greater bit depth, the images favor to become too large to transmit over a standard Internet connection. In order to display an image in a moderate amount of time, concept must be assimilated to reduce the image's file size. These concepts make use of mathematical formulas to analyses and compress image data, resulting in smaller file sizes. This method is called compression.

In images there are types of compression:

- Lossy compression.
- Lossless compression.

Both methods save storage space, but the operations that they tool differ. Lossy compression generates smaller files by rejecting excess image data from the original image. It discards details that are too small for the human eye to discriminate, resulting in close approximations of the original image, although not an exact copy. For example, an image format that uses this compression method is JPEG (Joint Photographic Experts Group).

Lossless compression, on the other side, never removes any information from the original image, but in place of represents data in mathematical formulas. The original image's virtue is maintained and the decompressed image output is bit-by-bit identical to the original image input. The most well-known image formats that use lossless compression is GIF (Graphical Interchange Format) and 8-bit BMP (Microsoft Windows bitmap file). Compression plays a very important role in choosing which steganographic algorithm to use.

4. Algorithm

Complexity of algorithm is depending on size of key and text. Pixel processing is converting our information in secret code encrypted the data in the image. Least significant bit for the patching of data due to the intensity of image is only converting into 1 and 0 after hiding the information. Convert in intensity is either 0 or 1 because change at last bit.

E.g., 11111000 is converted into
11111001.

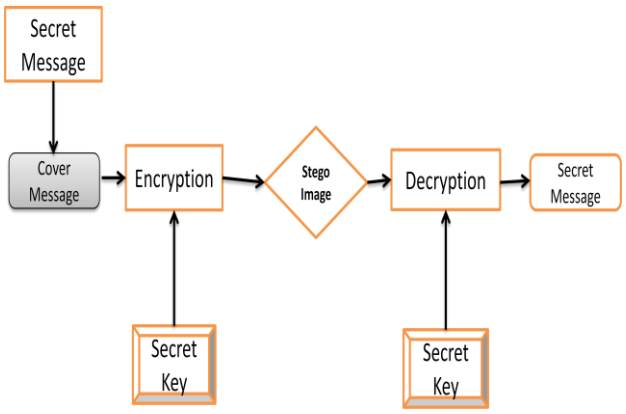

Fig.1: Cryptography flow chart

5. Cryptography Methodology:

- Normal text message:- Srihari
- Key:- Hello
- Convert the key and data in to ASCII format.
  E.g., Hello is converted to B [5]={8,5,9,9,13}.
  Srihari is converted to A[20]={19,18,9,8,1,18,9}.
- Pad the Normal message according to the length of the key.
  E.g., Srihari has 7 char.

In it and the key has letter, so first five letter of message will convert according to the key but in the end we have only two letter left so we pad p letter(x or y or z) for padding to make exact length paris.

Srihari sriharixxx

- A[20]={19,18,9,8,1,18,9,24,24,24}
- P = length of key
- Q = length of padded key

5.1 Encryption Algorithm

- Take two arrays flagkey and flagtxt of size of length of text and key and fill it with zeros.
- This process will be follows until the length of key.

Process for encryption of data by the key:

```
For k=1 to p
m=1
For i=1 to q
if(j>p)
{
j=1
r[i]=r[i]+s[j]
j++
```

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

```
 }
Else
{
r[i]=r[i]+s[j]
J++  }
End for
```

Process of hiding of key:

```
Do
for  j=1 to p-1
s[j]=s[j]+s[j+1]
end for
s[p]=s[p]+s[1]
End for
```

Convert the array A and B in to character form:

E.g.,

```
for  i=1 to q
while r[i]>256
{
r[i]=r[i]-256
flagtxt[i]+=1
}
end while
end for

For i=1 to p
while s[i]>256
{
s[i]=s[i]-256
Flagkey[i]+=1
    }
end if
End  for
```

6. Decryption Algorithm

This is reverse process of encrypted data.

Converting the encrypted data into ASCII format:

E.g., A[20]={22,144,31,234,256}
B[20]={11,3,233,20,25}

Decryption Process:

```
For  i=1 to q
While flagtxt[i]!=0
r[i]=r[i]+256
flagtxt[i]--
endwhile
endfor

for  i=1 to p
while flagkey[i]!=0
s[i]=s[i]+256
flagkey[i]--
End while
Endfor

for  k=1to p
s[p]=s[p]-s[1]

for  j=p-1 to 1
j=1

for  i=1 to n
If(j>p)
j=1
r[i]=r[i]-s[j]
end if

end for

end for
```

The larger the cover image is (in data content terms-number of bits) relative to the hidden text, the easier it is to hide the latter. For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media. It is not clear how commonly this is actually done.

For example: a 24-bitbitmap will have 8 bits representing each of the three colour values (red, green, and blue) at each pixel. For the blue alone, there will be 2^8 different levels of blue intensity. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used more or less undetectably for something else other than color information. If this is repeated for the green and the red elements of each pixel as well, it is possible to encode one letter of ASCII text for every three pixels**.**

7. Conclusion

This Paper gave an overview of Image steganography and different techniques its major types and classification for steganography which have been proposed in the literature are in above. We embedded the message into the images and its protected with the personal key. So it is not possible to damage the data by unauthorized person. The proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the message more secure. In image hiding, the secret data is concealed in cover image and the result is called a stego-image while its quality should be acceptable so as not to observe the attraction of other people. A Least significant bit embeds data in the LSB position of bit pixel of a cover image.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

8. Future Enhancement

The proposed approach in this paper uses a steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded and is protected with a password which is highly secured. LSB algorithm in this paper application is faster and reliable and compression ratio is moderate compared to other algorithm. It accepts only bit map image as a carrier file, and the compression depends on the document/carrier image size. The Future work is to improve the compression ratio. For more security use the asymmetric cryptography algorithm in steganography.

Researchers proposed many image hiding techniques based on LSB. A new method of LSB uses Genetic Algorithm (GA) in which the purpose of using GA is to find an optimal replacement of LSB in order to increase the imperceptibility. So, it is not possible to damage the data by unauthorized personnel. We are using the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithm.

References

[1] Krativyas, B.L.pal, "A proposed method in Image steganography to improve Image Quality with LSB technique", 2014.
[2] Jas,eetkaur, Nitikakapoor, "A Literature survey: Steganography using Redundant bit Replacement by Neural Network",2014.
[3] MeddiHussai, Mureed Hussain, "A survey of image steganography of basic techniques",2014.
[4] VikasTyagi, Atulkumar, Roshanpatel, " Image steganography using least Significant Bit with cryptography",2012.
[5] Namita Tiwari, Dr. Madhusandhilya, Dr. MeenuChawla, "Spatial Domain ImageSteganography based on Security and Randomization",2014.
[6] Mrs.Kavitha, KavitaKadam, AshwiniKoshti, PriyaDunghav,"SteganographyUsing Least Significant Bit Algorithm", 2012.
[7] Amirthanjan.R, Akila.R and Deepikachowdavarapu,"A Comparative Analysis of Image Steganography,2010.
[8] Bandyopadhyay.S.K., "An alternative Approach of steganography using the Reference Image", 2010.
[9] Mathkour, H., B. Al-Sadoon, and A. Touir ,"A New Image Steganography Technique Steganlayis concept",2008.
[10] Zanganesh.O, S. Ibrahim," Adaptive Image steganography Based on Optimal Embed & Robust Against Attack,",2011.

Revathi. R.R is holding the Under Graduation Degree in BCA (Computer Applications) from Alpha Arts and Science College and pursuing Post Graduation in Master of Computer Applications in S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report writing.

P. Tamilarasi is holding the Under Graduation Degree in BCA Computer Applications from Mahalashmi Women's College of arts and science and pursuing Post Graduation in Master of Computer Applications in S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report writing.

D. Vigneshwari is holding the Under Graduation Degree in BCA Computer Applications from Thirumurugan Women's College of arts and science and pursuing Post Graduation in Master of Computer Applications in S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report writing.