INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

COMPARISON OF VARIOUS STEGANOGRAPHY TECHNIQUES

Computer Science

Amandeep Kaur Guru Gobind Singh Indraprastha University, Guru Tegh Bahadur Institute of Technology, Rajouri Garden, New Delhi 11064, India

Anurag Sharma Guru Gobind Singh Indraprastha University, Guru Tegh Bahadur Institute of Technology, Rajouri Garden, New Delhi 11064, India

Anuj Sharma Guru Gobind Singh Indraprastha University, Guru Tegh Bahadur Institute of Technology, Rajouri Garden, New Delhi 11064, India

Gurjyot Singh Guru Gobind Singh Indraprastha University, Guru Tegh Bahadur Institute of Technology, Rajouri Garden, New Delhi 11064, India

Tanisha Jain Guru Gobind Singh Indraprastha University, Guru Tegh Bahadur Institute of Technology, Rajouri Garden, New Delhi 11064, India

ABSTRACT

There has been a need of communicating confidential information secretly since immemorial time. Moreover, even today it finds its applications in military and intelligence sharing. Although, cryptography can be used to encode the secret message into a form that cannot be understood by the attacker, but it can still be deciphered by the attacker using various cryptanalysis techniques. This is where the need of steganography arises. Steganography is an art of hiding secret message in a cover media like image, video, audio or speech etc. In this paper we have studied, implemented and compared various Steganography techniques available in image processing.

KEYWORDS

Steganography, Spatial Domain Method, Transform Domain Method, Least Significant Bit Substitution, Discrete Cosine Transform

1. Introduction

Stegano is Greek word which means sealed and graphy means secret writing thus making Steganography art of science whichs means covered writing (hide in plain sight) ,and over hundred years its techniques are being used. During transmission of data via channel, a trespasser may not be able to predict the presence of secret message beneath audio, video or text. Firstly, an encoder is used to encode message with media, thereby transmitting the media over channel and receiver decoding the media to obtain encoded secret message. Several steganography techniques are in the industry to use for such security purpose. The paper centres on the idea of studying, implementing, comparing various steganography techniques.

2. Related Work

In [1] Rejani.R, et.al 'Comparative Study of Spatial Domain Image Steganography Techniques' has overviewed about following steganography techniques in image processing Least Significant Bit Steganography ,RGB Steganography, Most Significant Bit Steganography Pixel Value Differencing Steganography Peak-Signal To Noise Ratio(PSNR) Steganography, Root Mean Square Error Steganography, Mean Squared Error Steganography

In [2] the author(s) have overviewed about following steganographic techniques in image processing; Least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations

In [3] Ramadan. Mstafa et.al 'Information Hiding in Images Using Steganography Techniques' has overviewed about following steganography techniques; Least Significant Bit, Discrete Cosine Transform, Discrete Wavelet Transform

In [4] Nick Nabavian 'CPSC 350 Data Structures: Image Steganography' has overviewed about following steganography techniques; Least Significant Bit

3. Implementation

This research paper will bolster various techniques, implementation, and comparison among them. Image steganography techniques can be classified into two broad categories [1]; spatial domain based steganography, transform domain based steganography

3.1 Spatial Domain Method

In spatial domain scheme, the secret messages are embedded directly. Various techniques in spatial domain method are:

- Least Significant Bit Substitution(LSB)
- RGB Substitution
- Redundant Pattern Encoding
- Encrypt And Scatter
- Masking And Filtering

3.2 Transform Domain Method

The transform domain Steganography technique is used for hiding a large amount of data with high security, a good invisibility and no loss of secret message. Various techniques in Transform Domain Method are:

- Discrete Cosine Transform
- Discrete Wavelet Transform

3.3 Techniques Used

In this research paper following techniques have been implemented

- Least Significant Bit Substitution
- RGB Substitution
- Discrete Cosine Transform

4. Least Significant Bit Substitution

It is the simplest and oldest method of image processing in steganography. In this technique the secret message is embedded into the digital cover image by modifying the least significant bit of the pixels of the cover image.

This method uses least significant bits for substitution so as to cause minimum distortion in the cover image .The LSB of some or all of the bytes inside an image is changed to a bit of the secret message. The choice of number of bits in the pixels of cover image to be substituted is made so as to make the stego image indistinguishable from the cover image. [1, 2, 3, 4, 6, 7]

```
def encode(cls, input_image_path, output_image_path,
 encode_text):
    """
    hide text to image
    :param input_image_path: str
 :param output_image_path: str
 :param encode_text: str
 """
 normalize(input_image_path, output_image_path)
hide_text(output_image_path, encode_text)
assert read_text(output_image_path)==encode_text,
read_text(output_image_path)
def read_text(path):
 """
read secret text from image
:param path: str
 :return: str
 """
 img = Image.open(path)
 counter = 0
result = []
for y in range(img.size[1]):
 for x in range(img.size[0]):
r, g, b = img.getpixel((x, y))
if is_modify_pixel(r, g, b):
 result.append(counter)
 counter += 1
  if counter == 16:
   counter = 0
 return to_str(''.join([hex(_)[-1:] for _ in result]))
def hide_text(path, text):
 """
hide text to image
  :param path: str
:param text: str
 """
 text = str(text)
# convert text to hex for write
write_param = []
base = 0
for _ in to_hex(text):
write_param.append(int(_, 16) + _base)
base += 16
 # hide hex-text to image
img = Image.open(path)
counter = 0
for y in range(img.size[1]):
 for x in range(img.size[0]):
  if counter in write_param:
   r, g, b = img.getpixel((x, y))
   r, g, b = modify_pixel(r, g, b)
  img.putpixel((x, y), (r, g, b))
  counter += 1
  # save
  img.save(path, "PNG", optimize=True)
```

5. Discrete Cosine Transform

It transforms image in spatial domain to frequency domain. In this technique data will be divided into some blocks often 8 by 8 or 16 by 16 blocks. Now applying discrete cosine transform on each block will convert the signal into high, middle, and low frequencies. Low frequencies are closest to original data whereas middle and high frequencies are more details of data (low frequency represents smooth region of the image whereas high frequency represents edges of the image). Hence, details frequencies (middle and high frequency) can be used as a host data or cover data to hide secret data on it.[3,5]

```
def greyencoding(self):
hidden_message=self.to_bit_generator(open("sample1.txt",
"r").read() * 10)
img=cv2.imread('original.png',cv2.IMREAD_GRAYSCAL
E)
 try:
 for h in range(len(img)):

 for w in range(len(img[0])):
  img[h][w] = (img[h][w] & ~1) | next(hidden_message)
 except StopIteration:
 print("No more rows")
 cv2.imwrite("output1.png", img)
```

6. Tools Required

For implementation pycharm3.6 (community version) is used.

7. Comparison among different Steganography Techniques

Results of LSB insertion and Masking and Filtering technique are compared, on the basis of robustness; tolerance to image compression, cropping; area used for storing secret message; suitability for lossy JPEG image.

Table 1: Comparison between LSB Insertion and Masking And Filtering Techniques

	LSB Insertion	Masking and Filtering
Robustness	Low	High
Tolerance to image compression, cropping	Low	High
Area used for storing secret message	Least Significant Bits of pixels (noise level of cover image)	Significant area (Integral to cover image)
Suitability for lossy JPEG Images	Low	High

Table 2: Comparison between DCT and LSB

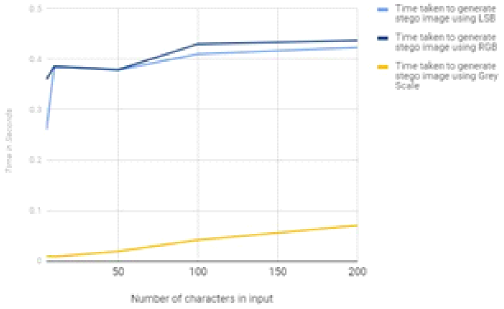
	LSB insertion	DCT
Type of Steganography	Spatial domain	Transform domain
Robustness	Low	High
Imperceptibility	Low	High
Embedding Capacity	Low	High
Tolerance to image compression and cropping	Low	High

7. Result

Here is a comparison among time taken in generating stego image by using LSB, RGB and Grey scale steganography technique.

Table 3: Comparison between LSB, RGB and Grey Scale

Number of characters in input	Time taken to generate stego image using LSB (in seconds)	Time taken to generate stego image using RGB(in seconds)	Time taken to generate stego image using Grey Scale(in seconds)
5	0.26	0.36	0.01
10	0.3853	0.3858	0.0093
50	0.378	0.379	0.02
100	0.41	0.43	0.042
200	0.423	0.437	0.071



Average time taken in case of LSB = 0.37126 s
Average time taken in case of RGB = 0.39836 s
Average time taken in case of Grey Scale = 0.03046 s

8. Conclusion

We have studied and implemented various steganography techniques using image. The choice of steganography technique depends upon the size and type of secret message, size of cover image and the level of security. LSB, DCT and RGB have been studied and implemented. Out of the three techniques i.e. LSB, DCT, and RGB, DCT is the fastest technique. LSB and RGB show similar behaviour till input length of is less than 50, on proliferation of character input LSB method appears to be better as compared to RGB method of steganography. However, DCT technique is fastest technique observed so far.

9. Future Scope

The following techniques can also be used in image steganography: Redundant Pattern Encoding, Encrypt and Scatter, Masking and Filtering, Discrete Wavelet Transform.

10. References

[1]. Rejani.R, Dr.D.Murugan,Deepu.V.Krishnan 'Comparative Study of Spatial Domain Image Steganography Techniques',Int. J. Advanced Networking and Applications Volume: 07 Issue: 02 Pages: 2650-2657 (2015) ISSN: 0975-0290 https://pdfs.semanticscholar.org/55f6/36074d7b848f25663697e59a035964871e26.pdf

[2]. 'The Types And Techniques Of Steganography Computer Science Essay' https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php

[3]. RamadhanJ. Mstafa, Christian Bach 'Information Hiding in Images Using Steganography Techniques', Conference: Conference: Northeast Conference of the American Society for Engineering Education (ASEE), At Norwich University David Crawford School of Engineeringhttps://www.researchgate. net/publication/259893801_ Information_Hiding_ in_Images_Using_ Steganography_Techniques

[4]. Nick Nabavaian 'CPSC 350 Data Structures: Image Steganography' http://www1.chapman.edu/~nabav100/ImgStegano/download/ImageSteganography.pdf

[5]. https://www.youtube.com/watch?v=Q2aEzeMDHMA&t=219s

[6]. https://www.youtube.com/watch?v=GNy_EjKs-6o

[7]. https://www.youtube.com/watch?v=VDUXeWu-GVo&t=32s