Image Steganography

Saketh Katari
Computer Science Department
IIIT-Delhi
Delhi, India
katari15045@iiitd.ac.in

***Abstract*—This document explains a new strategy to transfer confidential data by combining steganography with cryptography. LSB steganography is further improved by randomly storing confidential data in an image which makes it difficult to retrieve. Considering human visual system, it is difficult for the user to detect the changes in stego image.**

***Index Terms*—steganography, LSB, image, cryptography, random**

I. Introduction

Confidential data is everywhere and it is necessary to transfer it securely over internet. Cryptography comes into picture when the data is with you but nothing is made out of it, as it is a cipher, making no sense. Steganography hides confidential data within some other data (say image) and makes it difficult to even detect that there is a secret here. Cryptography combined with steganography provides a 2 layer protection - detecting the confidential data (steganography) and making sense out of it (Cryptography).

Images are used (among audio, video, text etc) as a medium to store the confidential data. Any data such as text, image, audio etc can be embedded in an image and is tranferred to the destination. If an attacker sees this image, it would be difficult to detect that there is some hidden data in it, as it looks lika a normal image.

II. Related work

Most of the traditional LSB steganography techniques store the confidential data in the LSBs (Least Significant Bit) of every pixel without any randomization. This is not secure because, an attacker might just access the LSBs of every pixel and retrieve the confidential data. Instead, some randomization is necessary while embedding data so that, when an attacker tries to retrieve data, it is difficult to produce the same pattern that was randomly generated.

However, it is necessary to transfer the random pattern to the destination to retrieve data that is embedded.

During the process of embedding data in an image, the LSBs of some pixels are modified which modifies the image [1]. As the LSB of any binary number corresponds to 0 or 1, it has very less effect (changes by 1) on the overall value.

The performance of a method or an algorithm is evaluated on the basis of the change in the image before and after embedding data in it. An algorithm is considered better if it produces minimal change in the image after embedding data in it.

III. Proposed model

This model adds cryptography and randomization to the traditional LSB steganographic techniques.

A. Notation

Cover_image - The image (before embedding) that is supposed to carry the confidential data in it.

Stego_image - The image (after embedding) that contains confidential data in it.

location_data - Meta data (Data about confidential_data) that identifies the location of confidential_data within a stego_image.

Component_of_a_pixel - The Red, Green and the Blue components (RGB).

LSB - Least Significant Bit of a binary number.

pr_key_src - Sender's private key

pr_key_dest - Receiver's private key

pub_key_src - Sender's public key

pub_key_dest - Receiver's public key

B. Pre-processing

A random location_data is generated with necessary length. Let it be 'abc'. This is converted to 8-bit ASCII values '97, 98, 99'. Finally, it is converted to a binary string '01100001, 01100010, 01100011'.

Similarly, another binary string is produced for the confidential_data.

C. Embedding

Each bit is taken from the confidential_data and from the location_data; let them be c_bit and l_bit respectively. c_bit is embedded in one of the components of a pixel which is determined by l_bit.

Fig. 1. Left - Cover_image, right - confidential_data_image [2].

It is observerd that the human eye is most sensitive to the green component of the light [2]. So, LSBs of green component are not replaced.

A pixel is chosen in lexicographical order (row_number, column_number in lexicographical order). For a given l_bit and c_bit, l_bit is XORed with LSB of green component. If it gives 0, LSB of blue is replaced with c_bit, else, LSB of red is replaced with c_bit [2].

Fig. 2. Left - Cover_image, right - stego_image [2].

As you can see in Fig.2, it is difficult to distinguish between the left (before embedding confidential_data) and right images (after embedding confidential_data)

D. Encryption

Stego_image is first encrypted by the pr_key_src and then encrypted with the pub_key_dest. pr_key_src is used as a digital signature. pub_key_dest makes sure that only destination can decrypt it with it's private key [2].

Similarly, location_data is encrypted.

Now, stego_image along with location_data is transferred to destination.

E. Decrpytion

Stego_image is first decrypted using the pr_key_dest and then with the pub_key_src. Now, the receiver has the decrypted stego_image .

Similarly, decrypt the location_data.

F. Extracting embedded data

A pixel is chosen in lexicographical order (row_number, column_number in lexicographical order). For each bit l_bit in location_data, XOR l_bit with the LSB of the green component. If it's 0, append the LSB of blue to the confidential_data, else, append the LSB of red to the confidential_data.

Convert confidential_data to 8-bit ASCII values and finally to ASCII characters.

G. PSNR (Peak Signal to Noise Ratio)

As name indicates, it is the ratio of signal and noise. Higher the PSNR lesser the noise in an image.

PSNR of traditional LSB based steganography techniques is around 53. This method gives a PSNR of around 56, better than traditional PSNR.

H. Security

It has two layers of security. First layer being steganography, second being cryptography.

It's difficult to detect whether there is confidential_data in an image. If an attacker somehow gets encrypted data, it's difficult to decrypt it.

IV. Conclusion

LSB steganography has been improved in three ways -

1. Two way security with cryptography.
2. It's difficult for an attacker to predict the random pattern that is used to embed confidential_data.
3. PSNR is increased from 53 to 56.

ACKNOWLEDGMENT

I would like to thank 'Technical Communication' staff and IIIT-Delhi (Indraprastha Institute of Information Technology).

REFERENCES

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A new approach for LSB based image steganography using secret key". Computer and Information Technology (ICCIT), 2011 14th International Conference, 22-24 Dec. 2011, Dhaka, Bangladesh.

[2] Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, "An improved method for LSB based color image steganography combined with cryptography". Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference, 26-29 June 2016, Okayama, Japan.