

Hide and Seek in JPEG Images

Medha Kulkarni

Dr. J. W. Bakal

ABSTRACT

Recently, the JPEG images are the most common format for storing images. JPEG images are very abundant on the Internet bulletin boards and public Internet sites. So it attracted the attention of researchers as the main steganographic format. There are many new and powerful steganography and steganalysis techniques in JPEG images reported in the literature, in the last few years. In this paper, steganography and steganalysis in JPEG is presented with F5 and JHRF-(JPEG information hiding algorithm of resisting F5) algorithms. F5 is one of information hiding algorithms based on the frequency domain. It has been widely used because of its high-capacity and robustness. JHRF is steganalysis algorithm based on frequency domain for F5. To deal effectively with abnormal data and to obtain better results, JHRF uses embedding secret information using some rules.

KEYWORDS-information hiding; steganography; DCT; F5; steganalysis

1. INTRODUCTION

Nowadays, there are many digital multimedia transmissions on the network. There could be some important data that need to be protected during transmission. Steganography is the art of invisible communication. Its purpose is to hide the presence of communication by embedding messages into digital cover objects. Now, invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages—digital documents, such as images, video, and audio files. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a cover object for hiding secret messages. Each steganographic communication system consists of an embedding algorithm and an extraction algorithm. To accommodate a secret message, the original image, also called the cover image, is slightly modified by the embedding algorithm. As a result, the stego image is obtained. Steganalysis is the art of discovering hidden data in cover objects. The set of stego images should have the same statistical properties as the set of cover images. If there exists an algorithm that can guess whether or not a given image contains a secret messages with a success rate better than random guessing, the steganographic system is considered broken. The

method is secure if the stego-images do not contain any detectable artifacts due to message embedding.

In the next section, we give a description of the JPEG image. In Section 3, we give the F5 algorithm theory. In section 4, we construct the JHRF algorithm, an attack on F5. The conclusion of paper is in Sect. 5.

2. JPEG

Joint photographic expert-group (JPEG) is a famous file for images. JPEG is an international standard for continuous-tone still image compression which has been approved by the ISO. It is the most common format for storing images, JPEG images are very abundant on the Internet bulletin boards and public Internet sites, and they are almost solely used for storing natural images.

Based on digital images (such as JPEG), information hiding is divided tow kinds of technology: space domain technology and transform domain technology. LSB substitution is commonly used in space domain technology. But LSB method's robustness is not well. Therefore, the researchers proposed some algorithms based on frequency domain. In recent years, there are some transform domain algorithms based on JPEG images, such as: J-Steg [3], F5[4], OutGuess[5]. Modern steganographic methods can also provide reasonable capacity without necessarily sacrificing security.

3. The F5 Algorithm

The F5 steganographic algorithm was introduced by German researchers Pfitzmann and Westfeld in 2001. The goal of F5 is to develop concepts and a practical embedding method for JPEG images that would provide high steganographic capacity without sacrificing security. Instead of replacing the LSBs of quantized DCT coefficients with the message bits, the absolute value of the coefficient is decreased by one. The F5 algorithm embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to embed a message of certain length.

F5 is enhanced version of F4 algorithm with respect to 2 main features stated below which help in preventing statistical attacks and improving embedding efficiency:

- PERMUTATIVE STRADDLING
- MATRIX ENCODING

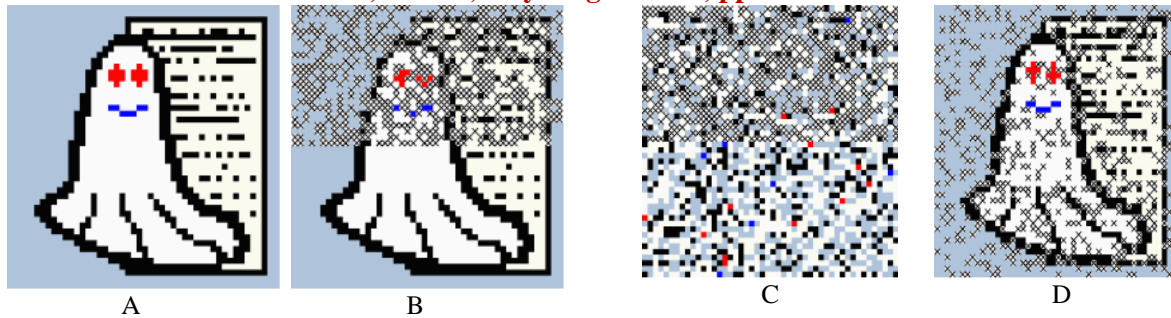


Fig 1: Continuous Embedding concentrates changes (x)

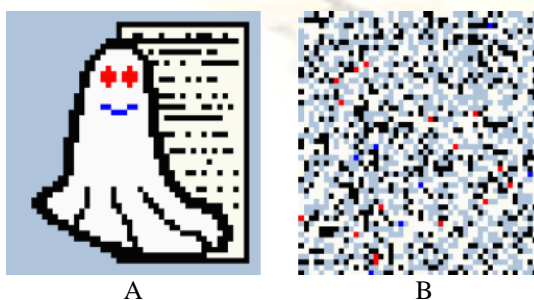
Continuous Embedding Problem:

In most of cases, an embedding message does not require full capacity. Hence a part of the file remains unused. Fig. shows this concept of continuous embedding used by algorithm like F4. Fig. 7 shows that changes (x) concentrate on the start of the file, and unused rest resides on the end. To prevent attacks, the embedding function should use the carrier medium as regularly as possible. The embedding density must be same elsewhere.

Per-mutative Straddling:

To prevent the Continuous Embedding problem discussed before, F5 algorithm uses a technique called Per-mutative Straddling for scattering the secret message over the whole carrier medium as shown in Figure 2(Treat each pixel as JPEG coefficient). The straddling mechanism used in F5 shuffles all coefficients using a permutation first. Then, F5 embeds into the permuted sequence. The shrinkage does not change the number of coefficients (only their values)The permutation depends on key derived from a password. F5 delivers the steganographically changed coefficients in its original sequence to the Huffman coder. With correct key,receiver will be able to repeat the permutation.

Fig 2 : Permutative Straddling scatters the changes (x)



According to the description of the F5 algorithm, version 11, the program accepts five inputs:

- Quality factor of the stego-image Q;
- Input file (TIFF, BMP, JPEG, or GIF);
- Output file name;
- File containing the secret message;
- User password to be used as a seed for PRNG;
- Comment to be inserted in the header.

In the embedding process, the message length and the number of non-zero non-DC coefficients are used to determine the best matrix embedding that minimizes the number of modifications of the cover-image. Matrix embedding has three parameters (c, n, k), where c is the number of changes per group of n coefficients, and k is the number of embedded bits. In their paper [16], the authors describe a simple matrix embedding (1, 2k-1, k) using a “hash” function that outputs k bits when applied to 2k-1 coefficients.

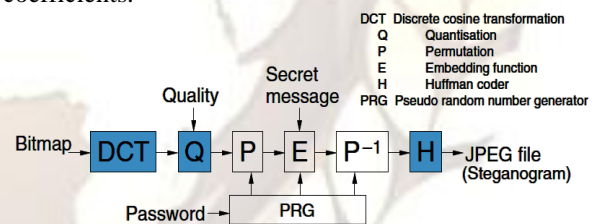


Figure 1 Model of F5 Algorithm

The embedding process starts with deriving a seed for a PRNG from the user password and generating a random walk through the DCT coefficients of the cover image. The PRNG is also used to encrypt the value k using a stream cipher and embed it in a regular manner together with the message length in the beginning of the message stream. The body of the message is embedded using matrix embedding, inserting k message bits into one group of 2k-1 coefficients by decrementing the absolute value of at most one coefficient from each group by one. The embedding process consists of six steps. The steps are mentioned below.

1. Get the RGB representation of the input image.
2. Calculate the quantization table corresponding to quality factor Q and compress the image while storing the quantized DCT coefficients.
3. Compute the estimated capacity with no matrix embedding $C = hDCT - hDCT / 64 - h(0) - h(1) + 0.49h(1)$, where hDCT is the number of all DCT coefficients, h(0) is the number of AC DCT coefficients equal to zero, h(1) is the number of AC DCT coefficients with absolute value 1, hDCT/64 is the number of DC coefficients, and $-h(1)+0.49h(1) = -0.51h(1)$ is the estimated loss due to shrinkage (see Step 5). The parameter C and the message length together determine the best matrix embedding.
4. The user-specified password is used to generate a seed for a PRNG that determines the random walk for embedding the message bits. The PRNG is also used to generate a pseudo-random bit-stream that is XOR-ed with the message to make it a randomized bit-stream. During the embedding, DC coefficients and coefficients equal to zero are skipped.
5. The message is divided into segments of k bits that are embedded into a group of $2k-1$ coefficients along the random walk. If the hash of that group does not match the message bits, the absolute value of one of the coefficients in the group is decreased by one to obtain a match. If the coefficient becomes zero, the event is called shrinkage, and the same k message bits are re-embedded in the next group of DCT coefficients (we note that $LSB(d) = d \bmod 2$, for $d > 0$, and $LSB(d) = 1 - d \bmod 2$, for $d < 0$).
6. If the message size fits the estimated capacity, the embedding proceeds, otherwise an error message showing the maximal possible length is displayed. There are rare cases when the capacity estimation is wrong due to a larger than anticipated shrinkage. In those cases, the program embeds as much as possible and displays a warning. While the F5 algorithm does modify the histogram of DCT coefficients, the authors show that some crucial characteristics of the histogram are preserved, such as its monotonicity and monotonicity of increments. The F5 algorithm cannot be detected using the χ^2 attack because the embedding is not based on bit-replacement or exchanging any fixed Pairs of Values.

4. JHRF

The principle of JHRF algorithm is to retain other AC coefficients of the same, only for the low-frequency region for 1 and -1 of the AC coefficients of embedding secret information, and reduce the changes of the AC coefficients by the use of matrix codes, embedding in the normal way and in the reverse. the number of 1 and -1 remains basically unchanged.

Encoding rules

Normal encoding rule

If Secret information is 1, the ac coefficient of frequency domain of the image is one. If Secret information s is 0, the ac coefficient of frequency domain of the image is negative 1.

$$ac = \begin{cases} 1, & \text{if } s = 1 \\ -1, & \text{if } s = 0 \end{cases} \quad (3)$$

Reverse embedded rule

If Secret information is 0, the ac coefficient of frequency domain of the image is one. If Secret information s is 1, the ac coefficient of frequency domain of the image is negative 1.

$$ac = \begin{cases} -1, & \text{if } s = 1 \\ 1, & \text{if } s = 0 \end{cases} \quad (2)$$

Extraction rules

An embedded part of the normal If the ac coefficient of frequency domain of the image is one, Secret information is 1. If the ac coefficient of frequency domain of the image is negative 1, Secret information s is 0.

$$s = \begin{cases} 0, & \text{if } ac = -1 \\ 1, & \text{if } ac = 1 \end{cases} \quad (4)$$

If the ac coefficient of frequency domain of the image is one, Secret information is 1. If the ac coefficient of frequency domain of the image is negative 1, Secret information s is 0.

$$s = \begin{cases} 0, & \text{if } ac = 1 \\ 1, & \text{if } ac = -1 \end{cases} \quad (5)$$

Demarcation point

The boundaries of an embedded part of the normal and reverse will determine the true value of its demarcation point. Let d is the difference of the number of ac coefficient of 1 and for -1. Then d is zero for the carrier image. As information is embedded in image, the process will cause the number of 1 and -1 change. d will not be 0. If you find a point of an embedded part of the whole divided into parts and in the reverse embedding embedded part, can make d remains 0,

or close to 0. Claimed that the point is the critical point. The following will be described

Computational Information
Systems6:1(2010) 55-62

MODEL OF JHRF ALGORITHM

The model of JHRF algorithm system is shown in Figure 1. It is the composition of the main embedding algorithm and the extraction algorithm. The part of embedding algorithm is divided into two parts. Normal encoding rule is used in one part. Reverse embedded rule is used in the another part.

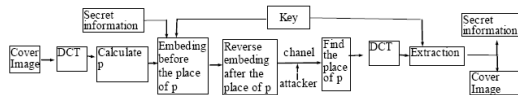


Figure 1. Model of JHRF

Embedding algorithm is described as follows.

- (1) Input cover image and the secret information is converted to bit-streams.
- (2) DCT transform of cover image and quantization of DCT coefficient.
- (3) Calculate p based on secret information and cover image.
- (4) Normal encoding rule is used before the place of p.

Reverse embedded rule is used after the place of p.

- (5) Cover image becomes stego image.

Extraction algorithm is described as follows.

- (1) Find the value of p.
 - (2) DCT transform of image.
- Normal Extraction rule is used before the place of p.
Reverse Extraction rule is used after the place of p.
- (3) Secret information is composed of bit-stream.

5. CONCLUSION

Thus F5 is effective method for embedding message into image. . The DCT transformation along with matrix coding is used to hide the data into it. It provides larger steganographic capacity in frequency domain The JHRF is steganalysis algorithm in steganography. It estimates the message length and effectively deals with abnormal data.

6. REFERENCES

- [1] Tang Ming-wei, Wang Guang-wei, Fan Ming-yu, Li Wei "An JPEG Information Hiding Algorithm of Resisting FR" IEEE Computer Society, 978-1-4244-5874-5/10
- [2] Westfeld A. F5-A Steganographic algorithm [C]//International Workshop on Information Hiding, LNCS Springer-Verlag, 2001, 2137:289-302.
- [3] Mingwei TANG,, Mingyu FAN, Wen SONG, YajunDU "A Steganalysis of Information Hiding For F5" Journal of

- [4] Tang Ming-wei, Wang Guang-wei, Fan Ming-yu "An Extential Steganalysis of Information Hiding For F5" IEEE Computer Society, 978-1-4244-5874-5/10

- [5] Hatim A. Aboalsamh Hassan I. Mathkour Mona F. M. Mursi Ghazy M.R. Assassa Steganalysis of JPEG Images: An Improved Approach for Breaking the F5 Algorithm 12th WSEAS International Conference on COMPUTERS, Heraklion, Greece, 2008

- [6] Jessica Fridrich1, Miroslav Goljan1, Dorin Hoge Steganalysis of PEG Images: Breaking the F5 Algorithm[C]. Proceedings of the 5th Information Hiding Workshop, Lecture Notes in Computer

- [7] Niels Provos Defending against Statistical Steganalysis [C] //Proceeding of the 10th USENIX Security Symposium. USENIX Press, 2001:323-335.

- [8] P Sallee, Model-Based Steganography [C]//Interntional Workshop on Digital Watermarking . Springer-Verlag 2004, 2939: 154 -167.

- [9] Manikopoulos C , Shi Y Q , Song S et al . Detection of block DCT2based steganography in gray2scale images. Multimedia Signal Processing , 2002 , 12 (1) : 3552358

- [10] Fridrich J, Goljan M, Hoge D. New methodology for breking steganographic techniques for jPEGS[C]. CA: Proc EI SPIE Santa Clara, 2003.143-155.

- [11] Fridrich J, Soukal D. Quantitative Steganalysis of digital images: Estimating the secret message length[J]. ACM Multimedia Systems Journal, 2003,9(3):288-302.