Study on Information Hiding Technology Based on Digital Image

Chen Chen  
Dalian Institute of Science and Technology, Dalian, China  
35765801@qq.com

Abstract. This paper introduces the basic knowledge of the digital image and information hiding technology, it is major to discuss about the embedding and abstracting process of hiding the digital file information, and the result of experiment has proved that information hiding has a better hiding effect; the examination of LSB information hiding technology, propose to compare secret information file’s bits with carrier image’s low bits, the success or failure of result is directly related to the effect of the hiding information. The experimental result shows that when the carrier image hide secret information, the quality of the image has a little change, and the size of the file is unchanging, and file summary is identical, moreover secret information can recover from carrier image perfectly; also shows that the LSB algorithm’s hiding effect, simplicity, safety of digital image information hiding.

1. Introduction
With the development of technology, digital multimedia is applied widely. Internet and wireless networks offer ubiquitous channels to deliver and to exchange information. The global communications capabilities of Internet not only bring people more convenience to share information, but also bring great danger and challenge to sensitive information and copyright. How to protect the information safety, will become the first problem to solve.

2. Digital Image
Human being can get about most of the information from visual, what’s more; the image can emerge in all kinds of styles: visual and non-visual, abstractive and physical. Windows uses bitmap file as standard image file formats. Image can divide into small area called pixel, in every pixel, expressing the data of brightness or color can be sampled and quantified, so that you can get the data of pixel. These pixels are displayed horizontally row by row. This process is called digitization, and the image we get is called digital image. Digital image can be divided into different file styles, for example TIFF, BMP, JPEG, JPG, PNG, and GIF and so on.

2.1. The color of digital image
The color is constituted by red, green and blue, any color can be made by the three primary colors (red, green, and blue) in deferent proportion [3]: The true color usually point that the proportion of RGB is 8: 8: 8, moreover, it is also called full color image. The false-color is not based on every color components, and it regards pixel data as the address entrance to the entry of color look-up table, to
search the number of R, G and B, to display images. **The gray scale images described one number corresponding of each pixel to its brightness.** Binary Image, the Intensity of each pixel can be ranged the value from 0 to 1.

### 2.2. Common type of digital image

![Figure 1. Color and Multispectral Images](image1) ![Figure 2. Gray Scale Image](image2) ![Figure 3. Binary Image](image3)

#### 3. Information Hiding Technology

Information hiding is technology system which is covered by many areas, much science (digital signal processing, Image Processing, Pattern Recognition, digital communication, multimedia technology, Cryptography, language processing and so on, perception physiology, psychology). The carrier that information carrier can carry is text, for example TXT, HTML, PDF, image, IP packet and so on. It takes use of Human organ system’s insensitive, and hides the secret information in a special carrier by some way, so that it cannot be awarded and noticed.

Information hiding is to hide the meaningful information into carrier message by some embedding algorithm, for example, software serial number, secret text and copyright information, so that we can get the process of secret carrier. Embedding algorithm is major to use the time redundancy and spatial redundancy of multimedia information, and people have an effect on masking of information changes. After information is hidden, unlawful users cannot confirm that whether other information is also hidden in the carrier or not, it is also difficult to abstract or delete the secret information that has been hidden. After secret carrier reaches receiver by the channel, receiver uses the key to recover or discover the hiding secret information by receiver’s detector.

The information hiding technology can solve safety problems, and there are two aspects: firstly, it can make medium information (non-secret information) known to public on the safety of copyright and using right; secondly, the secret information is safe during transmission and storing.

#### 3.1. The Characteristic of Information Hiding Technology

The **Information Hiding** has various features such as: Robustness, Undetectability, Capacity, Invisibility, Security, Self-repairability, and Symmetry.

#### 3.2. Information hiding based on Bitmap File

BMP image file is bitmap file, is the standard image style of Windows settings. Bitmap is constituted by several points, every point called pixel. So Bitmap file is also called raster image or pixel image. Every pixel has its own RGB number, and an image is a lattice which is constituted by a series of pixel points.

Digital colour images are typically stored in 24-bit files and use the RGB colour model. In a Bitmap file, true color bitmap file of 24 bits is widely used. A typical image file has two parts, the header and the raster data. The header contains the magic number identifying the format, the image dimensions, and other format-specific information that describes how the raster data relates to image points or pixels.

```c
typedef struct tagBITMAPFILEHEADER {
    WORD           bfType;
    DWORD     bfSize;
```
WORD  bfReserved1;
WORD  bfReserved2;
DWORD  bfOffBits;
} BITMAPFILEHEADER;

For example Fig.2 Gray Scale Image - bitmap file header structure:
00000000h: 42 4D 38 04 04 00 00 00 00 36 04 00 00 28 00;
00000010h: 00 00 00 02 00 00 00 02 00 00 01 00 08 00 00 00;
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00;
00000030h: 00 00 00 00 00 00 01 01 01 00 02 02;

Table 1. Header Structure of Bitmap File

| Name      | Offset | Data type | Length | Explain                              | Example Value | Examples of significant |
|-----------|--------|-----------|--------|--------------------------------------|---------------|------------------------|
| bfType    | 0      | WORD      | 2      | ASCII string "BM"                    | 42 4d         | BM                     |
| bfSize    | 2      | DWORD     | 4      | File Size                            | 00 04 04 38   | 263, 224 bit           |
| bfReserved1 | 6   | WORD      | 2      | Reserved position, 0                 | 00 00         | 0                      |
| bfReserved2 | 8   | WORD      | 2      | Reserved position, 0                 | 00 00         | 0                      |
| bfOffBits | 10     | DWORD     | 4      | Offset to image data                 | 00 00 04 36   | 1078 bit               |

Table 2. Analysis of image file’s header and the raster data

| Analysis                        | Value                  |
|---------------------------------|------------------------|
| The size of file                | 00240036h = 2359350 Bytes |
| The Offset of file              | 54 Bytes               |
| The bits per pixel              | 24 Bits                |
| Compression Type                | 0: No compression      |
| The size of Data image          | 2359350 − 54 = 2359296 Bytes |

3.3. LSB Hiding Technology

LSB is an easy method to embed secret information directly in the carrier image, which are used because people are visual redundant to visual image, and also use a special key to produce random signal by m sequencer, then according to certain rules, arrange two-dimensional watermark signal, embed secret information into the pixel points of carrier image to a place that is the least important bite, and to operate in a low position or the some lowest ones [4].

LBS uses secret bits of information to replace the least important bits, traditional LSB embedding are sequential embedding and embedding random intervals. The flat constituted by the lowest one or two bits of image pixel basically reflect noise, there is not too much information are useful for image. So traditional LSB algorithm is to embed 1 bit secret information in the lowest position of carrier element (or 2bit secret information in the two lowest position of carrier element). LSB has many advantages, for example, it is good for hiding, it has a large amount of information hiding and it is also easy to implement, so that it has been widely used.

3.4. Replace the LSB of the airspace based on Information Hiding

In this way, the lowest one or more bits plat of data part image pixel (carrier pixel) is replaced by hiding data. And at first LSB plat of carrier pixel is set zero, then according to the need, the hiding data will become one or not, so that it can hide data.
3.4.1. **Bitmap file the information embedded in the steps are divided into the following steps:**

1. The information that will be hidden turn into binary data stream;
2. The image data part of bitmap file will compare its every parity of each byte to the above binary data stream;
3. To change the parity of bytes by adjusting the lowest number 0 or 1 of the bytes, so that it will be identical to the above binary data stream, and embed information in the bitmap file of 24 bits.

3.4.2. **Hidden information extraction steps are as follows:**

1. to judge every parity of each byte of bitmap file image data part, if the amount of 1 in the byte is a even number, then print out 0, if the amount of 0 in the byte is an odd number, then print out 1;
2. 8 bytes for each judge, so that it will print out 8 numbers to constitute a binary (print out the high at first);
3. After the above treatment, you will get a series of 8-bit binary number, which is the code of hiding information, then the code will turn into text or image and voice, and you will get the information that had been hidden.

4. **Experimental Results**

4.1. **Experiment (I)**

LSB replacement steganography, **the basic idea:** To embed the secret information with the carrier to replace the image of LSB, the original image plane with the seven high-secret information on behalf of the LSB plane composed of secret images.

4.1.1. **Embedding process:**

1. Selected l (m) pixels based on the key k under c.
2. For each selected pixel gray value, if the LSB bits of information you want to embed the same, do not change; Otherwise, the next step;
3. Secret bits of information instead of the original gray value of the LSB, while the high-7 remains unchanged, the modified image is s.

4.1.2. **8-bit gray scale image plane of the binary image that:**

![Figure 4. 8-bit gray scale image plane](image)

**Table 3. The PSNR of image**

| Substitute Bit | No.0 | No.1 | No.2 | No.3 | No.4 | No.5 | No.6 | No.7 |
|----------------|------|------|------|------|------|------|------|------|
| PSNR (dB)      | 50.99| 45.33| 39.40| 33.31| 27.31| 21.30| 15.02| 8.95 |
This shows that the image replace every a high bit, PSNR value would fall about 6dB, the degree of distortion of the image after embedding secret information increases with high bit placed.

4.1.3. **Extraction process**: According to the information embedded in the key to find the pixels out of the pixel gray value of LSB, formed after the secret arrangement.

A 24-bit bitmap file consists of the 54-byte header and image data components, which cannot hide the header information; start from the 55th byte of image data can hide some information.

For example, the 24-bit bitmap file data like 01100110, 00111101, 10001111, 00011010, 00000000, 10101011, 00111110, 10110000, then the odd-even order of the bytes are: 0, 1, 1, 1, 0, 1, 1. Now if you need to hide the information of 92 and 92 into 8-bit binary is 01011100, compare these two series and find that the 3th, 5th, 7th and 8th bit are inconsistent, then modulate the parity of certain bytes of the 24-bit bitmap file data, make them into the same with 92 to 8-bit binary data.

The 3th bit: change 10001111 into 10001110, then the bytes change from the odd to even.

The 5th bit: change 00000000 into 00000001, then the bytes change from the even to odd.

The 7th bit: change 00111110 into 00111111, then the bytes change from the odd to even.

The 8th bit: change 10110000 into 10110001, then the bytes change from the odd to even.

4.2. **Experiment (II)**

In order to verify the performance of these algorithms, a simulation experiment was done, the experimental environment are Windows XP and Matlab7.0 [7]. Study, 24 true color standard Lean (512 * 512) image as a carrier image, as shown in the Vector map, the Secret information are secret images. Hided by LSB, the Vector images can completely hide the confidential information, the attacker cannot attack.

4.3. **Watermark embedding and extraction**

(1) Vector map file size 2359296 bytes, the maximum that can be embedded 587968 bytes of data. The document summary of confidential information is 5FF1B30549D4A86C913A8D9FD7629F28.

(2) The file after hiding information size 2359296 bytes, compared to the changes of the size of the images before and after embedded, there is no change.

(3) Summary of the calculation to extract the watermark Document: 5FF1B30549D4A86C913A8D9FD7629F28, compare the summary of the contents of the watermark document with the confidential information document before, the results are the same.

5. **Conclusion**

Based on LSB hiding, by a large number of bitmap files of different sizes and different document formats secret experiments, have been the same conclusion, which verifies the correctness and feasibility of LSB hiding. Theoretical analysis and practice show that the method has the practical feasibility of the application and better security. On the one hand, according to formulae of luminance, and the sensitivity of human eyes to different colors, we can substitute the information that would be hidden for the lower bits of the RGB brightness of the Pixel; on the other hand, we can minimize the difference of the absolute Pixels rather, change the lower k bits of the image according the difference
of the absolute Pixels. But for now the current situation, information hiding is not enough mature, LSB algorithm because that it is directly in the airspace of the secret information embedded in images, only suitable for digital still bitmap images, once the image is compressed, frequency-domain transformation and so on, it is easy to destroy the integrity of confidential information, making the LSB algorithm has many limitations. For example, in the case of humans can not perceive, to improve the capacity, robustness and anti-aggressive, for voice, video, digital watermarking technology of text and other issues yet to be continuing to explore and practice. With the advances in computer information technology, to against the endless stream of New Attack Algorithm, Information Hiding combination of encryption technology of information will become necessary technical support of the development of network security.

References
[1] M. Ramkumar, A. N. Akansu. Capacity estimates for data hiding in compressed images [J]. IEEE Trans. Image Processing, 2010, 10 (25): 12521263.
[2] H. Chen, R. S. Run, J.L. Lai, et al.. A novel visual secret sharing scheme for multiple secrets without pixel expansion [J]. Expert Systems with Applications, 2010, 37 (12): 7858-7869.
[3] Hui.Luo. A Secure Text-based Information Hiding Technique [J]. Computer Engineering, 2004, 30 (19): 95-97.
[4] RMoulin, J. A. O'Sullivan. Information-theoretic analysis of information Hiding [J], IEEE Transactions on Information Theory, 2003,49 (3): 563-593.