

A Study of Information Hiding Algorithm Based on the Human Vision

J. DENG

General Administration of Press and Publication of the P.R.China, BeiJing, P.R.China

Y. ZHONG & Z.H. WEI

Qingyuan Advanced Technical School, Guangdong, P.R.China

G. WEI

Wisetronic INC., Toronto, Canada

ABSTRACT: After studying how to embed the secret message into digital pictures by taking advantage of the gray scale sensitivity of human eyes, this paper discusses an improved LSB algorithm for information hiding algorithm, which is a typical algorithm for hiding secret message. The improved algorithm analyzes the ability of the human visual system, strengthens the security of the hidden message, and increases the information capacity while keeping the imperceptibility of the hidden images.

KEYWORD: information hiding; LSB algorithm; gray scale sensitivity; maximum grayscale offset

1 INTRODUCTION

1.1 Background of information hiding technology

Information hiding is the technology to embed the secret information into a cover data, and to make the secret information invisible. Information hiding utilizes the characteristic of the insensitivity of human sensory organs, hides information in the host information for encoding and transmission without discovery. Although there is a long history for the information hiding technology, the concept of information hiding was first documented in a paper by David Parnas, "On the Criteria to Be Used in Decomposing Systems Into Modules" published in the Communications of the ACM in December 1972.

Here let us see some interesting examples about the information hiding in the human history. The first recorded uses of information hiding can be traced back to 440 BC when Herodotus, an ancient Greek historian, mentions two examples in his stories. Demaratus, a king of Sparta from 515 until 491 BC in ancient Greece, sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand [1]. Another example also happened in ancient Greece. A message was tattooed on the shaved head of a person, hidden by the hair that afterwards grew over it, at last exposed by shaving the head again. The message allegedly carried a warning to Greece about Persian invasion plans. In World War II, hidden messages usually

were written by secret inks, under other messages or on the blank parts of other messages.

1.2 The model of information hiding

In 1983, Gustavus J. Simmons studied the information hiding technology used by prisoners, Alice and Bob, who wanted to escape from prison. Gustavus J. Simmons published an article, The Prisoners' Problem and the Subliminal Channel [2]. Here the figure 1 is a description for the prisoners' problem, which is a good model for information hiding.

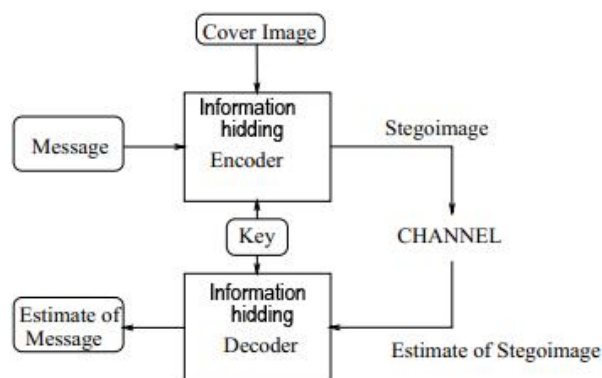


Figure1 A model of information hiding

Figure 1 includes both the embedding process and the extracting process for the information hiding. The embedding process is to hide the secret information into the open carrier by using an embedding algorithm. The extracting process is to recover the secret information by the reversed algorithm. From the model of information hiding,

we will know the carrier of secret information is usually open to everyone. This differs from cryptography in which communication is encrypted. The method of hiding information is to embed data imperceptibly, allow the data to be readily extracted, incorporate a certain amount of resistance to removal, and promote a high information rate or capacity [3][4]. The advantage of information hiding over cryptography is that messages do not attract attention to themselves.

1.3 Information hiding algorithms

Information hiding algorithms can be classified into spatial domain algorithm and transform domain algorithm.

1.3.1 Spatial domain algorithm

Human eye can not detect some small change of gray and color in pictures, because each human eye has about a limited number optic nerve cells so their ability to detect gray and color is limited. The spatial domain algorithm takes advantage of the characteristics of human vision. The popular algorithm on the spatial domain is LSB (Least Significant Bits) [5]. Experiment results show that with the method, good invisibility to the image can be achieved. Although calculation for the algorithm is simple and fast, it usually has low information hiding capacity and low security.

1.3.2 Transform domain algorithm

The principle of the algorithm, by selecting some specific parameters of the transform domain, is to spread hiding information to the whole image. Comparing with the regular spatial domain methods, it takes human visual and mental systems into consideration by decomposing original image to multi-resolutions in frequency domain. It provides ideal compression ratio, including JPEG image compression. Different experimental results show the hidden information capacity of this algorithm is much more than spatial domain algorithm, but its computing complexity is much more than the other one.

2 IMPROVED LSB ALGORITHMS

According to the sensitivity of the human eye to gray scale variations, we distinguish two similar images usually by the just noticeable difference of their gray level. Following is a description of the LSB algorithm and a study to improve it.

2.1 LSB algorithm and its shortcoming

LSB (Least Significant Bits) belongs to the spatial domain algorithm. LSB is a common, simple

approach to embedding information in a cover image. It works with the least significant bits of the pixel components in the image and changes them according to the message's bits to hide. The algorithm is to place the embedding data at the least significant bits (LSB) of each pixel in the cover image. Because human eye is less sensitive to LSB, altering LSB doesn't change the quality of image to human perception. And the converted image is sensitive to a variety of image processing attacks like compression, cropping etc.

On the basis of the traditional LSB algorithm and in light of the masking characteristics of the human vision system, only some least bits for all pixels are used to hide information in a host image. The image then is demarcated into the smooth area, edge area and texture area, and secret messages are embedded in the corresponding areas respectively. This may give the attacker an opportunity to discover the secret information by only decoding some fixed number of LSBs of the image pixels. To improve the algorithm, we have to spread the secret information to more bits.

2.2 The sensitivity of the human eye to gray scale variations

For a color picture, human eye is more sensitive on green and red components than blue channel. The position and capacity for information hiding can be considered by the value of luminance intensity is different for the RGB color vector in an image [6]. In the same way, we can also consider the position and capacity for information hiding because human eye has the sensitivity to gray scale variations.

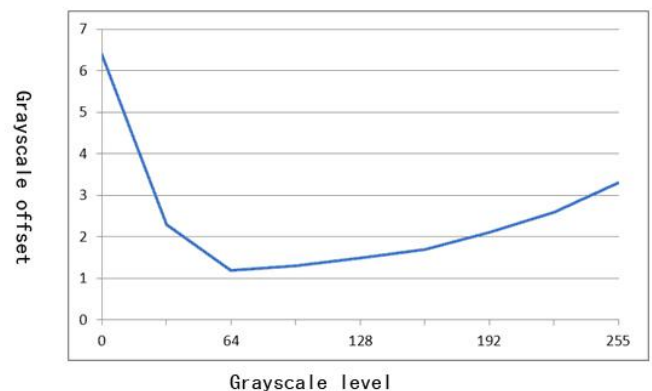


Figure2 Sensitivity of human eye to gray scale variations

Figure 2 reflects the ability of human vision to detect gray scale variation [7]. Assuming every pixel has 8 bit, the number of the gray-level will be $2^8=256$. By the picture, we can tell human eye can not distinguish one from the other in the interval [0, 3] and [224, 255]. For example, closing to the gray level 0, human eye can only distinguish the gray more than 7 level differences. But in the interval [64,

192], human eye can distinguish the gray with only 2 level differences. Based on this sensitivity of the human eye to gray scale variations, we may improve the LSB algorithm not only by increasing the least bits, but also take advantage of the bits of low-gray scale and high-gray scale simultaneously.

2.3 Improved LSB algorithm

To improve the traditional LSB algorithm, we achieve the highest hiding efficiency under the constraint of human visual perception. Our method tries to increase hiding efficiency with adaptive numbers of LSB according to the human visual system sensitivity to image contrast change.

Assuming the offset value for the maximum gray scale is d , the bit numbers to embed into the position is $K = \{k = \log_2 d (k \in N)\}$, the binary expression for the embedding information is m_k , the low bits for

the pixels of the original image is p_k , let us see the steps of embedding secret information.

Step A. Randomly process the secret information and convert it into streams of binary bits;

Step B. Reads the pixels' bits of the original image;

Step C. Use random value to calculate the coordinate of possible pixel for information hiding;

Step D. Based on the maximum offset d , calculate the bits number k for embedding information;

Step E. If $|m_k - p_k| \leq d$, then $k = k + 1$; Repeat the operation until $|m_k - p_k| > d$, then switch to next step;

Step F. Replace p_{k-1} by m_{k-1} . If the embedding process is done, switch to the last step, otherwise jump back to step C;

Step G. Export the image with secret information.

Following is the flowchart to explain the improved algorithm.

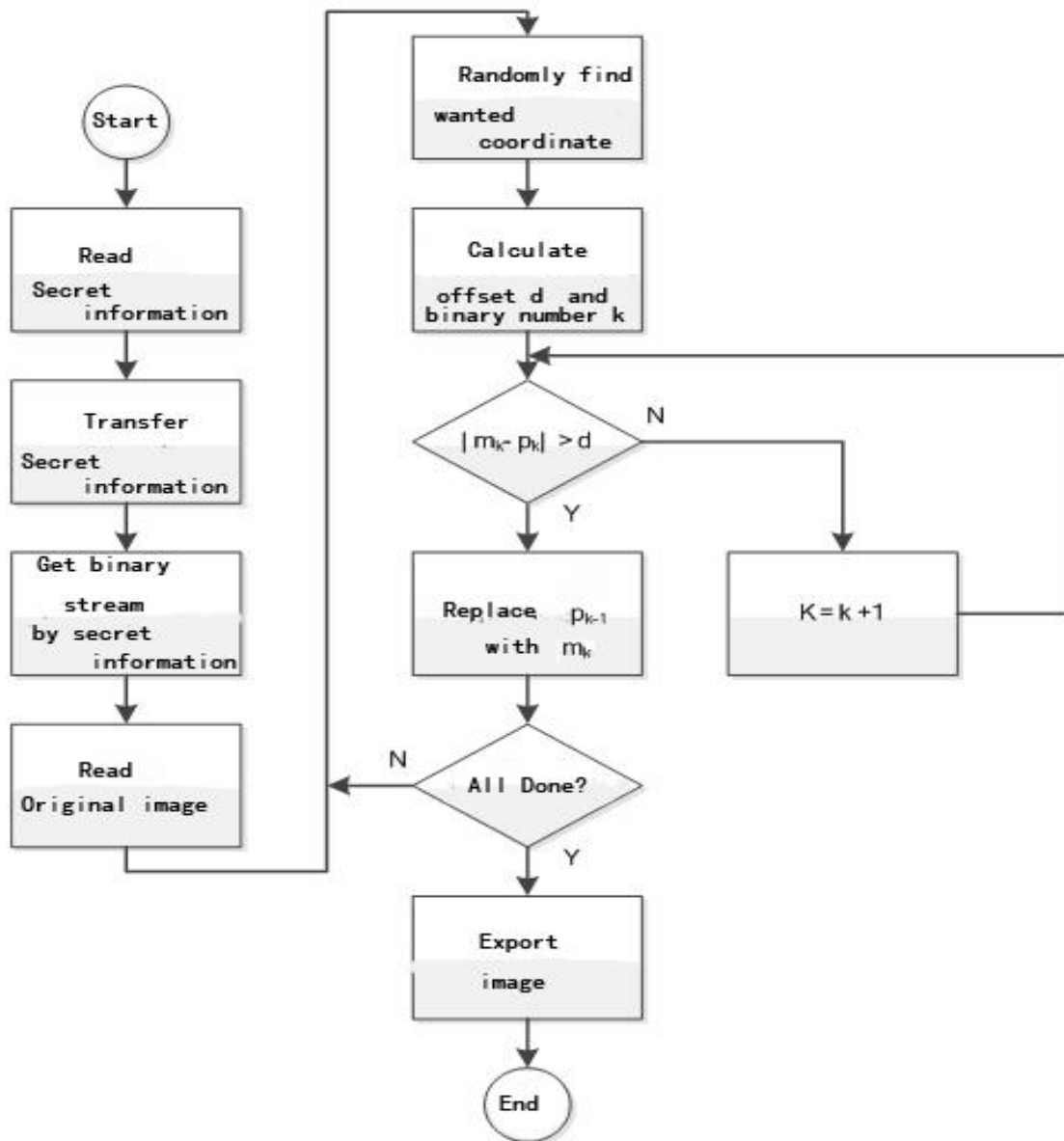


Figure 3 Flowchart for the improved algorithm

Here is an example.

First the secret information is randomly converted to a stream of binary bits.....11011101. Then one image as the host is imported.

Now it is the step C. The coordinate, (31,42), for the first chosen pixel is randomly chosen, its pixel value is 20(00010100). Based on figure2 its maximum offset $d=4$, and so the bits number to be convert is $k=2$ ($k = \log_2 4 = 2$).

If $k=2$, then the embedding information $m_2=01$, the possibly converted bits of the original image is two low bits $p_2=00$. Because $|m_2-p_2|=1<4$, the embedding process can be continued.

With the accumulation of K , $k=3$, $m_3=101$, $p_3=100$, $|m_3-p_3|=1<4$, the embedding process can be continued again.

Now $k=4$, $m_4=1101$, $p_4=0100$, $|m_4-p_4|=9>4$, there is no place to embed additional information. Replace p_3 with m_3 until the pixel value changed into 21 (00010101).

Repeat from the step C to find the next pixel in the original image and then continue the following steps.

Export the image with the embedding information until the whole embedding process is finished.

2.4 Strength of improved algorithm

Comparing with the traditional LSB algorithm, the improved one is more secure. Because the storage bits to embed secret information is decided by the gray-scale of the original image pixels, the secret information will not be hidden in some fixed bits. Normally the improved algorithm spreads the bits number to 3 or 4, while the regular algorithm uses only 1 or 2 bits. This increases both the capacity for hiding information in an image, information, and the security for the hiding.

3 CONCLUSIONS

With the rapid development of Internet technologies, the amount information sent and received electronically is increasing greatly. As the technology of transmitting information on network in secure, the importance of information hiding came to be recognized widely. This paper has proposed a novel method for embedding secret information into a host image subject to the constraint of human visual perception. The classical LSB method is adopted, but with adaptive numbers of LSBs to hide secret information. However, more experiments should be needed to analyze its efficiency and capability.

REFERENCES

- [1] Petitcolas FAP; Anderson RJ; & Kuhn MG. (1999). Information Hiding: A survey. Proceedings of the IEEE (special issue) 87 (7): 1062-78.
- [2] Simmons G. J. (1984). The Prisoner's Problem and the Subliminal Channel. Advances in Cryptology: Proceedings of CRYPTO'83. Plenum Press: 51-67.
- [3] Bender W., Gruhl D., Morimoto N., & Lu A. (1996). Techniques for data hiding. IBM Systems Journal, 35 (3&4).
- [4] Cox I.J., Kilian J., Leighton T., & Shamoon T. (September 1996). Secure spread spectrum watermarking for images, audio and video. Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, III: 243-246.
- [5] Bianchi G. (1996). Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802. 1 1 wireless LANs //Proceedings of IEEE PIM RC, Taipei, Taiwan: 407-411
- [6] Zhang X., Zhu Y., Sun R., & Liu P. (2012). Hiding method in color image based on bit plane (Photoelectron and Laser), 1092-1095. (in Chinese)
- [7] Yu T., & Dai J. (2008). A new technology to improve infrared image by integrating human vision (Infrared and Laser Engineering), 951-954. (in Chinese)