Estimating the Secret Message in the Digital Image

M. Sivaram, PhD
Assistant Professor
Department of Computer Networking
Lebanese French University
Erbil

D. Yuvaraj, PhD
Professor
Department of Computer Science
Cihan University
Duhok Campus

Amin Salih Mohammed, PhD
Dean, College of Engineering and computer Science
Lebanese French University
Erbil

V. Porkodi
Department of IT
Lebanese French University
Erbil

ABSTRACT
In this paper, a new method for estimating the secret message in the digital image. The actual concept involved in this paper is that the secret message is embedded into the cover image at random pixel in the last two positions of the LSB. Due to this technique, the length restriction of the LSB method of hiding the data is enhanced. Since the previous two bits of the Least Significant Bits are altered the possibility of having a substantial content of information is possible. This technique will overcome the problems faced by many other steganography techniques like LSB, Filtering, Masking, etc... In the face of having only short messages embedded into the image.

Keywords
LSB, Steganography

1. INTRODUCTION
Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. Stenography is often confused with cryptology because the two are similar in the way that they both are used to protect valuable information. The difference between the two is the steganography involves hiding information, so it appears that no data is hidden at all. It is the art of undetectable communication. It is the art and science of writing hidden messages. The purpose of steganography is to protect the very presence of communication by embedding messages into innocuous-looking cover objects, such as digital images. The secret message is embedded in the original cover image by making slight modifications to it. As a result, the steganography image is obtained. An essential requirement for a steganographic system is undetectability: stego images should be statistically Indistinguishable from cover images. In other words, there should be no artefacts in the stego image that could be detected by an attacker with probability better than random guessing, given the full knowledge of the embedding algorithm, including the statistical properties of the source of cover images, except for the stego key. The standard methodology followed in the LSB technique is to embed the secret messages in the cover image at random pixel selected, and the insertion of the secret message is done in LSB position of the pixel selected. But in our proposed system choose a random pixel in a cover image and in that take the last two bits for encrypting the data. So, the data length of the secret message can be extended.

2. METHOD DESCRIPTION
The insertion of the secret message into the cover image is done in many steps. The necessary steps involved in it are as follows,

2.1 Cover image selection
To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format; otherwise, the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit colour image, a bit of each of the red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. Thus, an 800 × 600-pixel image can contain a total amount of 1,440,000 bits (180,000 bytes) of secret data. Likewise a 1920 × 1440 pixel image can carry a total amount of 8,294,400 bits (1,036,800 bytes) of confidential data. The following table represents various resolutions in 24bit colour images in which the secret data can be embedded.

A general block diagram for cover selection is given in fig1, in which, after obtaining the stego image, Alice compares the stego and cover images in order to decide whether she would like to transmit the stego image, or opt to select an alternate cover image. By doing so, she could choose cover images with which the resulting stego image would be misclassified (i.e., false negative) by the steganalyzer. Therefore even in the presence of a powerful steganalyzer, she has improved her chances of going undetected.

2.1.1 Cover based
Independent of the embedding operation, properties of the cover image used, will affect the performance of steganalyzer. Below will review two of such features:

Changeable Coefficients are the set of coefficients which will be utilised by the embedding process. Since the message is fixed in the cover selection problem, images with the more significant number of changeable coefficient will relatively have a smaller number of changes induced by the embedding operation.

JPEG Quality Factor as have observed through experimentation, a continuation of our previous benchmarking study in [3], JPEG quality factor is inversely correlated with the performance of steganalyzers. In other words the higher the JPEG quality factor, the less is the performance of the studied steganalysis.

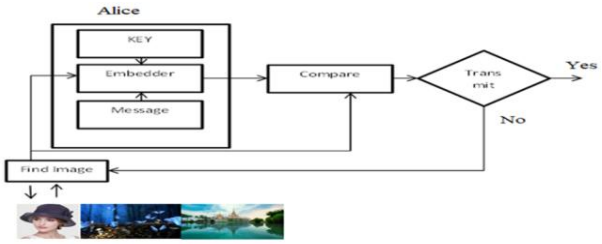

Fig 1: A block diagram for cover selection

2.2 Cover-stego based

Since it have available to us both the cover and stego images, it can measure the embedding artefacts directly. Thus, interested in measures which can quantify such artefacts. Below will introduce the cover-stego based measures which have employed in our work and motivate their selection:

Number of Modifications to the cover image could be thought as the most intuitive. The smaller the number of changes made the less detectable the resulting stegoimage should be.

Mean Square Error (MSE) is a simple non-perceptual error metric which is obtained from the cover-stego image pairs where lower MSE values are assumed to be indicative of lesser detectability.

Prediction Error is a local measure which have used in our experiments by looking at the difference between the mean prediction error of the cover and stego image using the prediction model proposed in [4]. Similar to MSE here prediction error is assumed to be correlated with detectability.

Watson's metric [5] is a perceptual measure, which is used in quantifying the quality of JPEG images. Therefore detectability should be lower as the difference in Watson's metric between the cover and stego is less.

2.3 Message Embedding

Let us consider an Image of size 800 x 600 colour image. In which every pixel consists of 24bits. The 24bit can be divided into three divisions 8 bits each. The first 8 bits are represented as RED; the second 8 bits are represented as GREEN, and the last 8 bits are designated as BLUE. So that a single bit is the combination of these three colours "RGB". This combination is shown below,

(00100111 11101001 11001000)

(RED GREEN BLUE)

The prevailing system in steganography LSB encryption technique says that the secret data will be encrypted into the pixel's Least Significant Bit (LSB) position. An alphabet can be embedded into the image by altering 3-pixel values.

Such as, when want to insert a character A into the image, have to convert the ASCII value of A into a binary value. The Binary value of A is 10000001. Consider three random pixels are selected as follows,

(00100110 11101001 11001000)

(00100110 11001001 11101000)

(11001001 00100111 11101000)

Diagram 1: Three original randomly selected pixels of an image.

In the LSB technique, the binary equivalent of the alphabet A replaces the least significant bits of the three selected pixels in the following way.

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

Diagram 2: Positions in which the binary values are changed

Resolution of cover Image	**Number of pixels**	**Number of bits**
800 x 600	480000	1440000
1024 x 768	786432	2359296
1280 x 1024	1310720	3932160
1600 x 1200	1920000	5760000
1920 x 1440	2764800	8294400

due to the insertion of the secret message.

In our proposed system, after choosing the random pixel in the image, the secret message can be inserted in the last two LSB position of the pixel as noted below.
(00100110 11101001 11001000)

(00100110 11001001 11101000)

(11001001 00100111 11101000)

Diagram 3: Three original randomly selected pixels of an image.

(00100110 11101000 11001000)

(00100101 11001001 11101000)

Diagram 4: Altered positions of the pixel in which the secret message is being embedded.

In the proposed technique it have inserted a character with the help of only 2 pixels instead of using the 3 pixels. So it can add more characters in a single image by using this technique.

While using a 24 bits image, it gives a relatively large amount of space to hide messages. It is also possible to use an 8-bit image as a cover source. Because of the smaller space and different properties, 8-bit images require a more careful approach. Where 24-bit images use three bytes to represent a pixel, an 8-bit image uses only one. Changing the two LSB of that byte will result in a visible change of colour, as another colour in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in grayscale, as the human eye will not detect the difference between different grey values as easy as in different colours.

In the olden technique, the main disadvantages of using LSB alteration are mainly in the fact that it requires a reasonably large cover image to create a usable amount of hiding space. Even nowadays, uncompressed images of 800 x 600 pixels are not often used on the Internet, so using these might raise suspicion. But in our proposed system it can overcome the problem by inserting a character in the last two bits of the bye.

2.4 Message Embedding and Extraction

Let s(k) 2 < denote a cover message, w(k) 2 < be the message carrier independent of the cover message and let the stego message be obtained as,

$y(k) = s(k) + hw(k)$; k = 1,2…..N

s(k) is continuous valued, and h > 0 denotes the message strength that could be adjusted based on perceptual characteristics, robustness properties etc.

Some of the w(k)'s (also continuous-valued) will be equal to zero based on the steganography key if that particulars s(k) does not carry a message bit. Assume s(k) and w(k) are samples from a stationary random vector. The steganography key and ® are known to the decoder. Suppose the decoder has access to the cover message s(k) then it is quite straightforward to extract the secret message by subtracting s(k) from y(k). On the other hand, if the decoder does have not access to s(k), then filtering techniques can be employed to obtain an estimate of s(k) and hence an approximate version w(k) which can then lead to bit errors.

3. CONCLUSION

The prescribed system is much more advantageous than the prevailing system. The main difficulty of selecting the cover image and the short secret message was enhanced in order to increase the holding of large messages into the cover image. Another additional feature is that the number of pixels that has to be used to embed the secret message into the cover image was reduced and the number of bits in the cover image's pixel that has to be altered is also reduced. This shows the efficiency over the other existing systems.

4. REFERENCES

[1] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, vol. 16(4), pp. 474−481, 1998.

[2] R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques", Proc. of ICIP 2001, Thessaloniki, Greece, October 7–10, 2001.

[3] S. Dumitrescu, Wu Xiaolin, and Zhe Wang, "Detection of LSB Steganography via Sample Pair Analysis", In LNCS vol. 2578, Springer-Verlag, New York, pp. 355–372, 2003.

[4] H. Farid and L. Siwei, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines", In LNCS vol. 2578, Springer-Verlag, New York, pp. 340–354, 2003.

[5] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compatibility", SPIE Multimedia Systems and Applications IV, Denver, CO, August 20−24, 2001.

[6] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images", Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, pp. 22–28, 2001.

[7] N. Provos and P. Honeyman, "Detecting Steganographic Content on the Internet", CITI Technical Report 01-11, 2001.

[8] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems", In: LNCS vol.1768, Springer-Verlag, Berlin, pp. 61−75, 2000.

[9] Steganography software for windows, http://members.tripod.com/steganography/stego/software.html