

Steganography in Images by Using Intersecting Planes

Esraa Jaffar Baker*

Received on: 26/10/2010

Accepted on: 7/4/2011

Abstract

Steganography is the art of hiding, and transmitting information using apparently innocent carrier without expose any suspicion. In this paper the proposed system is an implementation of image steganography techniques. This system will be used for embedding a steganography string into an image, which is true color image by using LSB technique to embedding text. The proposal technique is depending on the selection of the pixels that uses geometrical mathematical for intersecting planes. In this method the message cipher are repeated many time this help us to increased secure message. This method tests by many images, and give the results without distortion the image steganography.

Keywords: steganography, plane, information hiding

أخفاء المعلومات في الصور باستخدام تقاطع المستويات

الخلاصة

الكتابة المغطاة تعرف على أنها فن أخفاء المعلومات المرسلة، في نوافل بريئة المظهر وبدون إثارة الشكوك. في هذه المقالة النظام المقترن هو تنفيذ تقنيات أخفاء معلومات الصورة. وسوف نستخدم في هذا النظام تضمين سلسلة أخفاء معلومات في صورة، وهي صورة ملونة حقيقية وباستخدام تقنية الجزء الأقل أهمية (LSB) لتضمين النص. التقنية المقترنة تعتمد على اختيار نقطة ضوئية (pixel) وباستخدام هندسة الرياضيات لتقاطع المستويات. في هذه الطريقة الرسالة المشفرة تتكرر عدة مرات وهذا يساعدنا على زيادة أمنية الرسالة. هذه الطريقة اختبرت على عدة صور، واعطيت نتائج دون تشوهية صورة الأخفاء.

1. Introduction

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret [1]. Even if some un-authorized person can get the encrypted messages, he or she cannot understand the information without the key. However, cryptography may not be

Secure because it tells the attacker clearly that some secret messages are contained in the data. Usually, the encrypted messages look very unnatural. Some malicious person or group may just concentrate on the unnatural parts, and use all computing resources to decrypt the messages. Thus, to make the information more secure, some other technology is required [2]. An alternative technology is information hiding. Digital watermark and steganography are two representative technologies for information hiding [3].

Steganography is the art and science of communication in a way which hides the existence of the

communication. Also steganography focuses on undetectable communication, while watermarking focuses on reliable transmission of the message. The goal of watermarking is to protect copyrighted multimedia files [4]. Watermarks or copyright notice are used to identify the file as an intellectual property. They both differ in purpose, specifications and detection/extraction methods [5]. In watermarking, the object to be transmitted is the cover signal and embedded data which provides copyright protection. In steganography, the object to be transmitted is the embedded message and the cover signal that serves as a carrier. Therefore, watermark can be visible and there is no need to hide the presence of a watermark. Removal of a watermark renders the host signal useless. So, robustness against malicious attack and signal processing is a primary concern for watermarking. The necessary condition for a steganographic algorithm is to avoid the detection of the embedded message algorithmically or with the help of senses [6].

2. Information Hiding Component

We review the essential functional components of basic reversible information hiding system components, consider that an encoder consists of a cover image C (which acts as a carrier), and the message M is the data that a sender wishes to communicate confidentially. M can be plain/cipher text, images, or anything that can be embedded in a bit stream which is showing in Fig (1). The cover image C is used to embed the message by using a reversible data hiding technique controlled by stego-key K . K is a shared secret with the intended recipient whose knowledge

of the key enables them to decode the message from the stego-image. In the most general sense, a stego-key can be derived from the design parameters of a particular steganographic method used for embedding information [7].

The stego-key is the algorithm itself. The resulting stego-image obtained after embedding information is represented as $S=f(C,M,K)$. S is transmitted over a channel to the receiver where it is processed by the stegodecoder using the same key K . An interceptor of the stegoimage is expected to only see the innocuous image without any obvious indication of the embedded hidden message. Recovering the hidden message M and original image ' O ' from stego-image S . the decoding model is similar to encoding, which is shown in Fig (2).

3. Steganography based on Spatial LSB Replacement

(Least significant bit) LSB steganography is the most classic and simplest steganographic techniques, which embeds secret messages in a subset of the LSB plane of the image. A large number of popular steganographic tools, such as S-Tools, Steganos and StegoDos, are based on LSB replacement in the spatial domain [8]. LSB steganography can be described as follows:-

LSB insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800×600 pixel image, can thus store a total amount of

1,440,000 bits or 180,000 bytes of embedded data.

Although the number was embedded into the first 8 bytes of the grid. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. The human eye cannot perceive these changes, thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [9].

4. Compute the angle between two Planes

To specify a plane is to identify it in a way that makes it unique. One way is to set up an equation in a frame that will identify every point that belongs to the plane. There are several ways of specifying a plane, we will only mention four of them here, and the rest will be cases that we address in some problems later.

1- A plane can be defined by three non-collinear points.

2- A plane can be defined by two intersecting straight lines.

3- A plane can be defined to be perpendicular to a certain direction and at a specific distance from the origin.

4- A plane can be defined by being drawn through a given point and perpendicular to a given direction.

A direction, for our purposes, can be defined by a vector. In the case of a plane, the vector determining the direction is perpendicular to the plane and is said to be Normal to the plane.

To obtain an equation for a plane, we suppose that a point $P_1(x_1, y_1, z_1)$ on the plane and a nonzero vector $N = A_i + B_j + C_k \dots\dots\dots(1)$

Fig (3) shows the vector which is perpendicular to the planes, Then the point $P(x,y,z)$ will lie in the plane if and only if the vector $\overrightarrow{P_1P}$ is perpendicular to N ; that is, if and only if

$$N \cdot \overrightarrow{P_1P} = 0, \dots\dots\dots(2)$$

Or

$$A(x - x_1) + B(y - y_1) + C(z - z_1) = 0 \dots\dots\dots(3)$$

Equation (3) may also be written in the another form

$$Ax + By + Cz = D, \dots\dots\dots(4)$$

Where D is the constant $Ax_1 + By_1 + Cz_1$.

Conversely, if we start from any linear equation such as eq (4), we may find a point $P_1(x_1, y_1, z_1)$ whose coordinates are:

$$Ax_1 + By_1 + Cz_1 = D \dots\dots\dots(5)$$

Then, by subtraction, we may put the given eq(4) into the form of eq(5) and factor it into the dot product

$$N \cdot \overrightarrow{P_1P} = 0, \dots\dots\dots(2)$$

With N as is eq(1). This says that the constant vector N is perpendicular to the vector $\overrightarrow{P_1P}$ for every pair of point P_1 and P whose coordinates satisfy the equation. Hence the locus of points $P(X, Y, Z)$ whose coordinates satisfy such a linear equation is a plane, and the vector $Ai + Bj + Ck$, having the same coefficients that x, y , and z have in the given equation, is normal to the plane[10].

Example

Find the angle between the two planes $2x + y - 2z = 5$ and $3x - 6y - 2z = 7$

Solution: clearly the angle between two planes shown in Fig(4) is the same as the angle between their normals (actually there are two angles in each case, namely θ and $180^\circ - \theta$) form the equation of the planes we may read off their normal vectors:

Then

$$\cos \theta = \frac{A1 \cdot B2}{\|A1\| \|B2\|} = \frac{4}{21}, \theta = \cos^{-1} \left(\frac{A \cdot B}{\|A\| \|B\|} \right)$$

$\theta \approx 79^\circ$ (7)

5. Embedding Method

The proposed system is an implementation of image steganography techniques. This system will be used for embedding a steganography string into an image, which is BMP file format image by using LSB technique to embedding text. The proposal technique is depending on the selection of the pixels that uses geometrical mathematical for intersecting planes, the technique can be described in algorithm (1).

6. Extraction Text Steganography

In this method we extraction bits steganography with out using the original image, we need only know the length of bits hide in steg_image to extracted it. These bits hide with bits steganography, the technique can be described in algorithm (2).

7. Experimental Results

In this algorithm implements into many images, this result for one image by this method, the original

image and image after embedded steganography, The imperceptibility of steganography is measured by the steganography image quality in term of Peak-Signal-to-Noise Ratio (PSNR) (in dB). Most common difference measure between tow images is the mean square error. The mean square error measure is popular because it correlates reasonably with subjective visual tests and it is mathematically tractable. The quality measure of PSNR is defined with,

$$PSNR = 10 \log_{10} \left(\frac{I_{\max}^2}{MSE} \right) dB$$

Where max I is equal to 255 for 8 bit gray scale images. The MSE is calculated by using the Eq. (2) given below:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (Y_{i,j} - S_{i,j})^2$$

----- (10)

M and N denote the total number of the pixels in the horizontal and the vertical dimensions of the image. $S_{i,j}$, represent the pixels in the original image and $Y_{i,j}$, represent the pixels of the steg-image, the results shows in table(1).

Simulations are conducted on the images shown in the table (1). The simulations were realized for 5 different images of embedding and use data payload 400 bits. The message information is embedded only in the last bit (LSB) of the cover image. In the other realizations, the message information is embedded in the last bit of the cover image randomly. As can be seen embedding information into cover image causes some distortions.

From figures (5) and (6) the value of PSNR are sufficiently high in Sold, Light and Flower image , while MSE

is very low in these images. So this algorithm has created minimum disturbance to host image and perceptually both the images are alike.

8. Conclusions

There are number of conclusions were noticed from:-

- 1- We conclude the increasing in the iteration of steganography text for ten times the security is increased.
- 2- The proposed system gives us the random location of steganography text in different test images.
- 3- The criteria of accuracy of steg_image acceptable because the PSNR values are high and MSE is low values, it means low distortion.
- 4- More security can be gain when we used subset of XOR operations.

References

- [1]. T. Morkel, J.H.P. Eloff and M.S. Olivier., "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA), Research Group Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa, 2005.
- [2]. S. Venkatraman, A. Abraham, and M. Paprzycki, "Significance of Steganography on Data Security" Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Vol.2, 2004.
- [3]. Hiroyuki Nakamura and Qiangfu Zhao," Information Hiding Based on Image Morphing", Department of Information Systems Graduate School of the University of Aizu, Aizuwakamatsu, Fukushima, Japan 965-8580, IEEE 2008.
- [4]. H. Berghel and L. O'Gorman, "Protecting Ownership Rights Through Digital Watermarks" IEEE Comput., vol. 29, pp. 101-103, 1996.
- [5]. H. Wang and S. Wang, "Cyber Warfare: Steganography vs. Steganalysis" in Communications of the ACM, vol. 47, pp. 76-82, 2004.
- [6]. Gopalakrishna Reddy Tadiparthi and Toshiyuki Sueyoshi" StegAnim-A Novel Information Hiding Technique using Animations", Manuscript received May 25, 2006.
- [7]. Santosh Arjun and Narasimha Rao," An Approach to Reversible Information Hiding for Images", IEEE Members, India, 2009.
- [8]. Tao Zhang, Yan Zhang and Xijian Ping and Mingwu Song" Detection OF LSB Steganography Based on Image Smoothness", Dept. of Information Science, Zhengzhou Information Science and Technology Institute, P.R.China 2NLPR, Institute of Automation, Chinese Academy of Sciences, Beijing, China Dept. of Training, Zhengzhou Information Science and Technology Institute, P.R.China, 2006.
- [9]. Samir Kumar Bandyopadhyay and Indra Kanta Maitra," An Application of Palette Based Steganography", Dept of Computer Science & Engineering, University of Calcutta, India, International Journal of Computer Applications (0975 – 8887) Volume 6– No.4, September 2010.
- [10]. Thomas, "Calculus and Analytic Geometry", 4th edition, 1968.

Input: input original color image and steganography text

Output: steg_image

Step1: find the pixels that choice to hide data in it by using the many steps below:

Step1-1: calculate width for color image

Step1-2: take two lines from original image and calculate summation of two lines.

Step 1-3: to begin in random start we find random pixel by using equation

starting=summation mod 0.5 width(8)

(Condition we starting from three lines and above)

Step1-4: calculate the angle θ by using the equation (7) (where θ : is value between two pixels (A and B))

Step 1-5: to limiting the component save data we using less than effect to image, therefore we calculate summation for red, green and blue components to choice one for them to hide data in it, the less component is choice to hide data in even pixel in it.

Step 1-6: take odd pixel in two planes and find θ between them, therefore finds to all planes in image.

Step 1-7: calculate average of θ between two planes

If $\begin{cases} \theta > \text{average} \text{ then hide data in even pixel that in less line by using LSB} \\ \theta < \text{average} \text{ then hide data in even pixel that in greatest line by using LSB} \\ \text{otherwise } \theta = \text{average no state} \end{cases}$

Step2: embedding process: in this step, we take third line to save the iteration of steganography text for ten times and calculate the total of text after that hide in image with text in less component by using LSB and using subset XOR operations i.e. subset between one bit from text steganography with L.S.B. from less components of third line image.

Input: steg-image and length of bits hide in steg_image

Output: steganography text

Step1: in steg_image find the pixels that choice to hided data in it by using the many steps below:

Step 1-1: calculate width for steg_image.

Step 1-2: take two lines from steg_image and calculate summation of two lines.

Step 1-3: to begin in random start we find random pixel by using equation (8)
(Condition we starting from three lines and above)

Step1-4: calculate the angle θ by using the equation (7) (where θ :is value between two pixels (A and B))

Step 1-5: calculate summation for red, green and blue components to choice one for them to hide data in it, the less component is choice to hide data in even pixel in it.

Step 1-6: take odd pixel in two planes and find θ between them, therefore finds to all planes in image

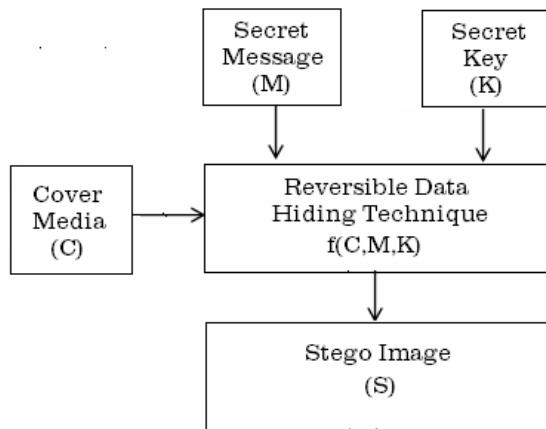
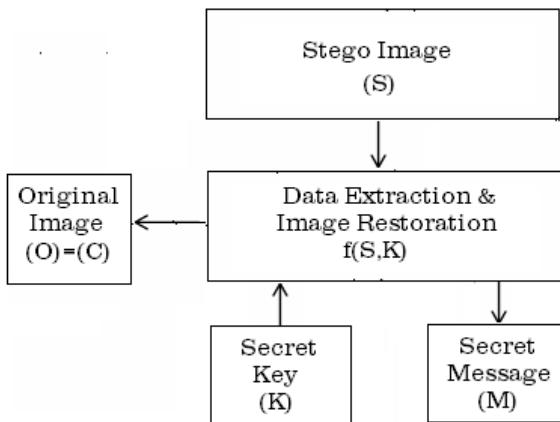
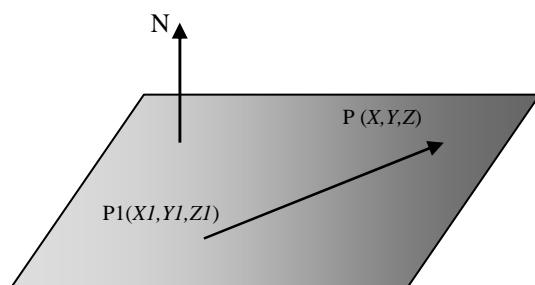
Step 1-7: calculate average of θ between two planes

$$\begin{cases} \theta > \text{average} & \text{then hide data in even pixel that in less line by using LSB} \\ \text{If } \theta < \text{average} & \text{then hide data in even pixel that in greatest line by using LSB} \\ \text{otherwise } \theta = \text{average} & \text{no state} \end{cases}$$

Step2: extraction process: in this step the extract text steganography form pixel by using mod by two operations then take remainder (0 or 1) from less components of third line image, then summation this bits to consist texts and stop extraction depending on length of bits of steg_image.

Table (1) shows: Original Image, Steg-image and PSNR

Image name	Original Image	Steg- image	PSNR(dB)	MSE
Sold			55.5	0.078
Fruit			49.89	0.098
Light			53.56	0.088
Flower			51.56	0.091
Bear			48.94	0.094

**Figure (1) Basic reversible information hiding system encoder****Figure (2) Basic reversible information hiding system decoder [7]****Figure (3) P lies in the plane though P1 perpendicular to N if and only if**

$$\vec{N} \cdot \vec{P_1 P} = 0,$$

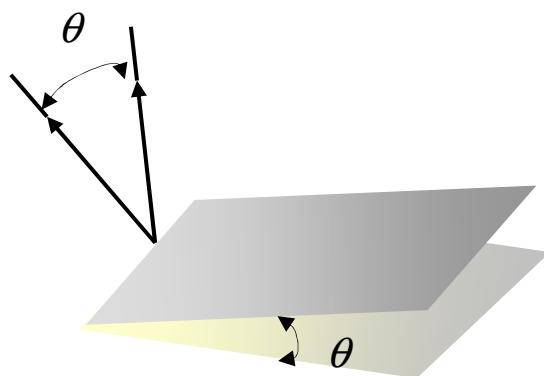


Figure (4) an Angle θ between Two Planes

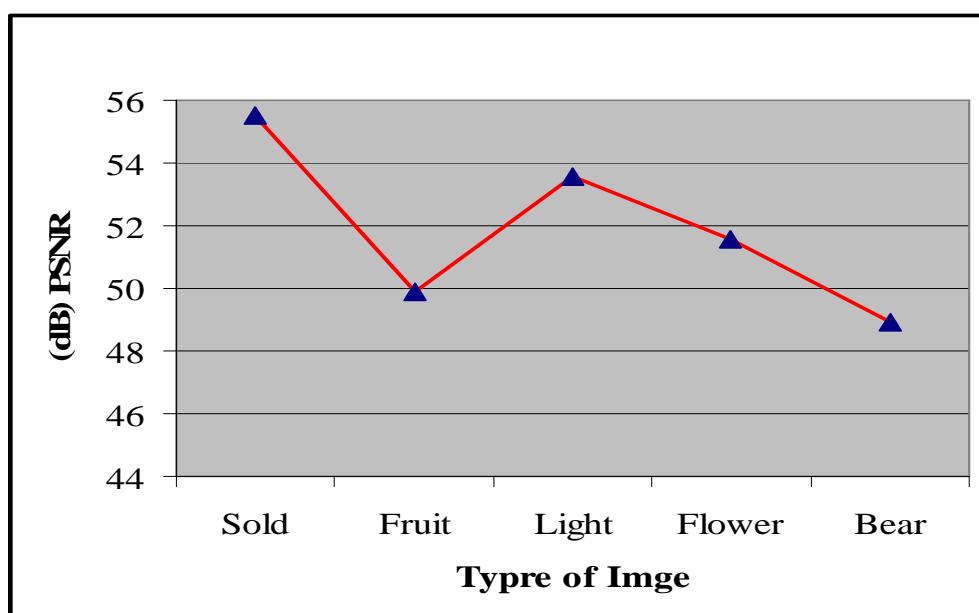


Figure (5) PSNR for Steganography in Images

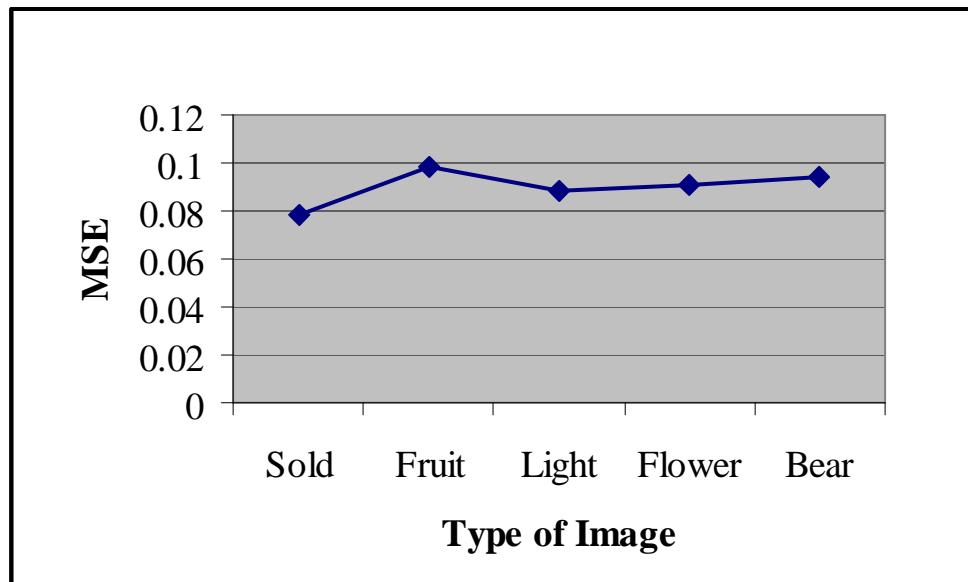


Figure (6) PSNR for Steganography in Images