Image Hiding Using Variable Length Least Significant Bits Embedding

Dr. Abbas A. Jasim

University of Basrah
College of Engineering
Computers Engineering Department

Abstract

In this work a new hiding system is proposed. It is based on Least Significant Bits (LSB) embedding of secrete image into another cover image.

The proposed hiding algorithm embeds the secrete image bits in the least significant bits of the cover image pixels such that the number of secrete image bits that are embedded in least significant bits of cover image pixel is variable and determined randomly. Such cover image pixel may contain no secrete information bit, one bit, two bits , or three bits according to the pseudo random number generator that generates integer numbers randomly between 0 and 3. The resulting image (the cover image within which the secret image is hidden) is called stego_image. Stego_image is closely related to the cover image and does not show any details of the secret information. It ensures that the eavedroppers will not have any suspicion that message bits are hidden in the image. The proposed system achieves perfect reconstruction of the secret message.

إخفاء الصور باستخدام تضمين الثنائيات الأقل تأثير متغير الطول

د. عباس عبد الأمير جاسم

جامعة البصرة–كلية الهندسة– قسم هندسة الحاسبات

الخلاصة

يتضمن البحث تصميم نظام جديد لإخفاء الصور السرية معتمد على تضمين الثنائيات الأقل أهمية بحيث يتم إخفاء بيانات الصورة السرية في الصور ذات التدرج الرمادي بحيث يكون عدد ثنائيات الصورة السرية المضمنة في كل نقطة صورية من الصورة الغطاء متغير يحسب عشوائيا بالاعتماد على مولد أرقام عشوائية. و بهذا فان أي نقطة من نقاط الصورة الغطاء قد لا تحتوي على ثنائيات عائدة للمعلومات السرية أو قد تحتوي على ثنائية واحدة، ثنائيتين، أو ثلاث ثنائيات منها. وذلك بالاعتماد على سلسلة الأرقام الشبه عشوائية المولدة. تسمى الصورة الناتجة بالصورة المختزلة و هي عبارة عن الصورة الغطاء بعد إخفاء المعلومات السرية بداخلها. تكون الصورة المختزلة مشابهة جدا للصورة الغطاء بحيث تضمن عدم إثارة شك المتطفل الخارجي بوجود بيانات سرية مضمنة. وكذلك فان هذه الطريقة تضمن عدم تمكن طرق الكشف من تخمين مكان وجود البيانات السرية أو عدد الثنائيات السرية المضمنة في كل نقطة من نقاط الصورة الغطاء. فيما يحقق نظام الإخفاء المقترح استرجاع تام للمعلومات السرية.

1. Introduction

Information security is becoming more important in data storage and transmission. Images are widely used in several processes. This makes protection of image data from unauthorized access to be strongly important [1]. The development of Internet provides a new way for digital information which can be made spreading faster and more conveniently. Because of the characteristic of digital images, some security problems come out besides the extensive usage of these images. [2]. Techniques and applications for information hiding have become increasingly more sophisticated and widespread as a solution of image security problem. Such applications include military and intelligence communication, covert private communication, and the protection of civilian speech against opponents [3].

Information hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright [3]. It refers to the nearly invisible embedding of information within a host data such as text, audio, image or video [4]. The process of hiding secret information in a manner such that the existence of secret information is concealed is called stagenography [5].It prevent outside observer from recognizing that hidden information is present. If a steganography method causes someone to suspect that there is secret information in the carrier medium, then this method fails [6]. So that hiding a message with stagenography reduces the chance of secret information being detected [7]. With high-resolution digital images as carriers (covers), detecting the presence of hidden messages has become considerably more difficult and messages embedded into an image are often imperceptible to the human eye [8][9]. Secrete data are generally embedded within insignificant area of cover image. Least significance bits of the original cover image pixels can be replaced with the secret image bits and the resultant image is not distorted. Since changing the pixel values by a small amount will not be noticeable [10].

Least significant bit (LSB) embedding is very frequently used in data hiding and there are many existing data hiding techniques to insert the secret data into the least insignificant bits (LSB) of the cover image [11][12][13]. They used LSB embedding replaces fixed number of bits of the cover image pixels with the secret information. The proposed hiding algorithm embeds the secrete image bits in the least significant bits of the cover image pixels such that the random number of secrete image bits to be embedded in least significant bits of cover image pixel. Matlab 2008a software is used to perform the proposed hiding system.

2. Gray Scale Images Format

Gray scale image structure represents images in a manner so called intensity image. In which image is represented as a data matrix of (M×N) elements. Each element of the matrix is corresponding to one image pixel. The elements in the intensity matrix represent various intensities, or gray levels. For eight bit pixel encoding, 0 represents black, while intensity level 255 usually represents full intensity, or white. Values within (0,255) range give the gray level of that pixel.

3. Key Generation Algorithm

Key stream is used for encryption to encrypt information. But in the proposed approach key stream is used for hiding information. It is used here as random number for allocating the secret image bits in cover image and to determine the number of bits to be embedded in each cover image pixel. The key stream is a well known in encryption especially for stream cipher. One way for its use in encryption is done by making bitwise XOR function between the plain text and the key [14].

Linear feedback shift registers (LFSRs) are widely used in key stream generators because they are well-suited for hardware implementation, produce sequences having large periods and good statistical properties. A (general) feedback shift register (FSR) of length L consists of L stages $[s_0, s_1, \ldots, s_{L-1}]$ (or delay elements) numbered 0, 1, …, L − 1, each capable of storing one bit. FSR having one input and one output, and a clock which controls the movement of data. During each unit of time the following operations are performed:

(i) The content of stage 0(s_0) is output and forms part of the output sequence;
(ii) The content of stage i is moved to stage i − 1 for each i, 0< i < L ; and
(iii) The new content of stage L − 1 is the feedback bit $s_j = f(s_{j-1}, s_{j-2}, \ldots, s_{j-L})$.
Hence, if the initial state of the LFSR is $[s_0, s_1, \ldots, s_{L-1}]$, then the output sequence $s = s_0, s_1, s_2, \ldots$ is uniquely determined by the recursion: $s_j = f(s_{j-1}, s_{j-2}, \ldots, s_{j-L})$ for j>L-1. The feedback function f is determined as :

$$f = (c_1 s_{j-1} \oplus c_2 s_{j-2} \oplus \ldots \oplus c_L s_{j-L}) \quad \ldots (1)$$

where each of the coefficients Ci is constant either 1 or 0 ,
f : is the feedback function which is a Boolean function, and
s_{j-i} : is the previous content of stage L_i.

For non zero initial function and primary feedback function, the LFSR will produce a pseudo random sequence of bits with period 2^{L-1} [12]. The block diagram of LFSR is shown in Figure 1.

4. The Proposed Hiding System

Information hiding is performed by replacing fixed number of least significant bits (LSB) of each data unit at the cover media sequentially in the scan lines across raw cover media format with the secrete information bits. An attacker can recover the hidden message by repeating the process many times. The proposed hiding approach improve the hiding security by making the secret image bits to be hidden are embedded as variable length chunks of bits distributed randomly by a pseudo random number generator (PRNG) across cover image. So that cover image pixel may contain no secrete information bit, one bit, two bits , or three bits according to the pseudo random number generator PRNG that generates numbers randomly between 0 and 3. In the proposed hiding system a key stream is generated and used as mask to distribute the secret image bits in the cover image and to determine the number of bits to be embedded in each cover image pixel.

4.1 The Procedure of the Proposed Hiding System

The steps of the proposed hiding approach are:

1- Generate the secrete key using the predefined key stream generators that are previously used for encryption. The key in this step is in the form of bit stream.
2- Decode the secret key as two bits numbers by taking each two adjacent bits and replace them by their decimal value called PRN (Pseudo Random Number). For example :
K = 110010011101
PRN = 3 0 2 1 3 1
3- Arrange the resulting RNG in two dimensional form to produce Random Number Generator RNG(i,j) matrix. Such that RNG has (M×N) numbers as the same as the image. The

arrangement is implemented by take the first N numbers of 1-D RNG to form the first row of 2-D RNG then take the next N numbers of 1-D RNG to form the second row of 2-D RNG and so on.

4- Use the RNG to allocate and distribute the secret bit on the cover image. As if RNG (i , j)=0, then no bit from the secret information will be embedded in pixel (i , j) in the cover image. If RNG (i , j)=1 then one bit of the secrete message bits will be inverted and replaced with the least significant bit of pixel (i , j) in the cover image. If RNG (i, j) =2, two bits of the secrete image bits will be replaced with the two least significant bits of pixel (i , j) in the cover image. And if RNG (i, j) =3, then three bits of the secrete image bits will be inverted and replaced with the three least significant bits of pixel (i , j) in the cover image.
5- Step 4 is repeated until all secret image bits are embedded in cover image. And the result is the stego_image that is the cover image within which the secret image is embedded.

4.2 The Procedure of the Reconstruction

The reconstruction steps, that reconstruct the secret image from the stego_image, are:

1- Generate the secrete key using the same algorithm used in the hiding process.
2- Decode the secret key as two bits numbers by taking each two adjacent bits and replacing them by their decimal value.
3- Arrange the resulting RNG in two dimensional form to produce RNG(i,j) in the same way of hiding process.

4- Use the RNG to extract the secret information from the stego_image. As if RNG (i , j)=0, then pixel (i , j) in the cover image contain no secret information bit. If RNG (i , j)=1, then one bit from the secret image will be extracted which is the least significant bit of pixel (i , j) in the cover image. If RNG (i , j)=2, then two bits from the secret image will be extracted which are the two least significant bits of pixel (i , j) in the cover image. And if RNG (i , j)=3, then three bits from the secret image will be extracted which are the three least significant bits of pixel (i , j) in the cover image.
5- Step 4 is repeated until all secret image bits are extracted from the stego_ image.
6- Rearrange the extracted bits in the original secret image form to obtain the reconstructed image by taking each eight consequent bit to form one pixel of the reconstructed image.

Figure2 shows the block diagram of the proposed hiding system.

5. Metrics

Several measurements are used to evaluate the performance of the proposed approach including energy, mean square error, correlation, and peak signal to noise ratio.

Image energy is used as one metric measure the similarity between the cover image and the stego_image resulting from hiding a secret image within cover image. Energy is also used to measure the similarity of the original and reconstructed secret image. The equation that was used in evaluating the energy E of a given image I of size MxN is [9]:

$$E = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} I^2(r,c) \qquad \dots (2)$$

The Mean Square Error (MSE) is used as a metric to measure the distortion between the resulting stego_image and the original cover image and between secret and reconstructed image. MSE is evaluated as [15]:

$$MSE = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} [I_1(r,c) - I_2(r,c)]^2$$

. ……..(3)

Where:
MSE: Mean Square Error
I_1: is the Image,
I_2: is modified image,
And M×N: Is Image size in pixel.

On the other hand, the correlation between an image I_1 and its modified version I_2 is given by the following equation[16]:

$$corr = \frac{\sum_{r=1}^{N} \sum_{c=1}^{M} (I_1(r,c) - \bar{I}_1)(I_2(r,c) - \bar{I}_2)}{\sqrt{[\sum_{r=1}^{N} \sum_{c=1}^{M} (I_1(r,c) - \bar{I}_1)^2][\sum_{r=1}^{N} \sum_{c=1}^{M} (I_2(r,c) - \bar{I}_2)^2]}}$$

……..(4)

where,
$\bar{I}_1$: image 1 mean
$\bar{I}_2$: image 2 mean

Another factor is used to evaluate the hiding system that is Peak Signal to noise ratio PSNR. This factor measure how the cover image get distorted by the hiding system [17]. PSNR is calculated as:

$$\text{PSNR} = 10 \times \log_{10} \frac{(2^r - 1)^2}{\text{MSE}} \quad \text{... (5)}$$

Where:
r: is the number of bit per pixel in each of cover image and stego_image that is 8 in this work.

6. Results and Discussion

The procedure of proposed hiding system is applied using gray scale cover image of size (256×256) pixels and gray scale secret images of size (128×128). The proposed procedure is applied on several cover and secret images arranged in five groups two of them are shown Figures 3 and Figures 4. The secret image is to be hidden in the cover image of the same group. First the PSNR is generated and PRN is formulated. The calculated mean value for PRN is found to be about 2. Accordingly, cover image size must be at least four times the size of the secret image. Table 1 listing MSE between stego–image and cover image, cover image energy, stego-image energy, and peak signal to noise ratio of the stego-image. While Table 2 shows MSE and correlation between secrete image and reconstructed image, secret image energy, and reconstructed image energy.

7. Conclusions

The proposed image hiding system implement secret image hiding system. The secrete image bits are embedded in the least significant bits of the cover image pixels such that the number of secrete bits to be embedded in least significant bits of cover image pixel is variable and determined randomly. So that cover image pixel may contain no secrete information bit, one bit, two bits, or three bits according to the pseudo random number generator that generates numbers randomly between 0 and 3. For this reason, it provides high level of security since external eavesdropper can not estimate the location of secrete information bits nor the number of secret information bits that are embedded within any cover image pixel. The result stego_image is less distorted and is very close to the cover image so that outside observer has on suspicious that the hidden (secret) information is present. This is obvious from Table 1 results, since energy values of stego image is very close to that of cover image, MSE has very small value, correlation factor is close to 1, and large value of PSNR.

The proposed approach ensures pefect reconstruction of secret image since correlation factor between secret and reconstructed images is exactly 1, MSE between secret and reconstructed images is exactly 0, and both secret and reconstructed image have the same energy value.

8. References

[1] Lala Krikor et al, "Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research, vol. 32, no. 1, pp 47-57, 2009.

[2] Hongxing Yao and Meng Li, "An Approach of Image Hiding and Encryption Based on a New Hyper-chaotic System",,vol. 7, no. 3 pp. 379-384, 2009.

[3] W. Bender , W. Butera , et al , "Applications for data hiding", IBM Systems Journal ,Vol. 39, pp 547-568,2000

[4] W. Niblack, et al., "The QBIC project: querying images by content using color, texture, and shape," Proc SPIE, Storage and Retrieval for Image and Video Database, vol. 1998, pp. 173-187, Feb. 1993.

[5] R. Chandramouli and N. Memon, "Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2001

[6] D. Artz, "Digital Steganography: Hiding Data within Data" ,IEEE Internet Computing, pp. 75-80, May-June 2001.

[7] F. N. Jhonson , Z. Duric , and S Jajodia , "Information Hiding : Steganography and Water Marking Attacks and Counter Measured", Klwer Academic Publishers,2001 .

[8] N. Provos. "Defending against statistical steganalysis. In 10th USENIX Security Symposium", Washington, DC, 2001.

[9] A. Westfeld and A. P_tzmann." Attacks on steganographic systems. In Proceedings of Information Hiding", Third International Workshop, Dresden, Germany, 1999.

[10] Min Wu, and Bede Liu "Data Hiding in Binary Image for Authentication and Annotation", IEEE Transaction on Multimedia, pp 528-538, August 2004.

[11] W. Bender, et al., "Techniques for Data Hiding", Proc. of SPIE Conf. on Storage and Retrieval for Image and Video, Vol. 2420, pp. 40, Feb. 1995.

[12] N. Nikolaidis, I. Pitas, "Copyright Protection of Images using Robust Digital Signatures", Proc. of, IEEE Int. Conf. on Acoustics, Speech, Signal Processing, Vol. 4, pp. 2168-2171, May 1996.

[13] P.H.W. Wong, O.C. Au, et al., "Image Watermarking Using Spread Spectrum Technique in Log-2-Spatio Domain", Proc. of IEEE Int. Sym. on Circuits & Systems, Jun. 2000.

[14] Varsha Bhatt et al., "Implementation of New Advance Image Encryption Algorithm to Enhance Security of Multimedia Component" , vol. 2, no. 4, pp. 13-20, 2012.

[15] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography" , CRC Press, 1996.

[16] H. H. Al _Obaidy ,"Encryption Using Wavelet Coded Image Data", MSc Thesis, Computer Engineering Department, College of Engineering ,University of Basrah,2004.

[17]Chin-Chen Chang., "A Fast and Secure Image Hiding Scheme Based on LSB Substitution", International Journal of Pattern Recognition and Arti_cial Intelligence , vol. 16, no. 4, pp. 399-416, 2002.

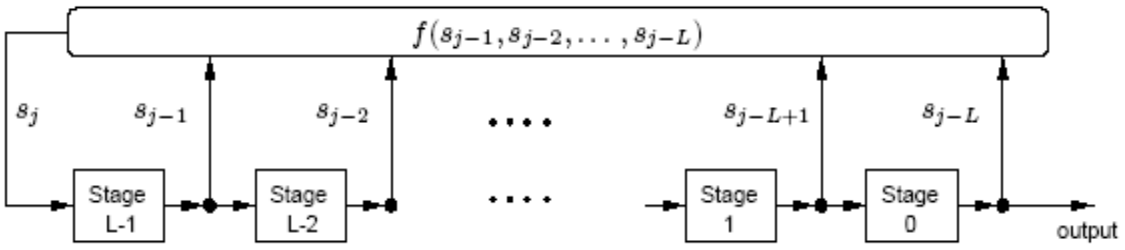
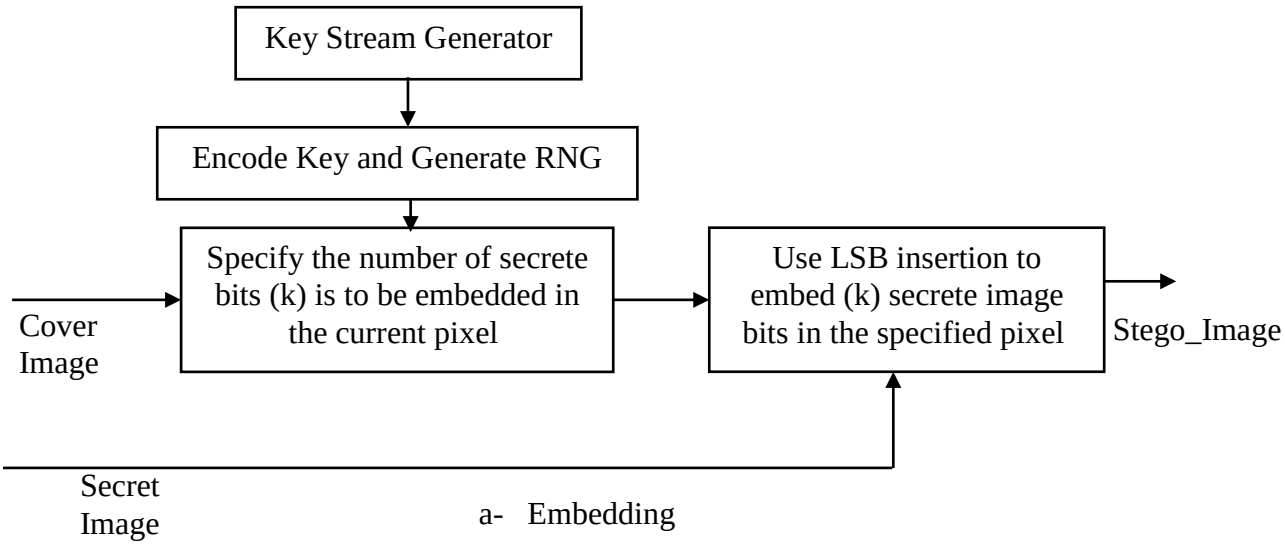
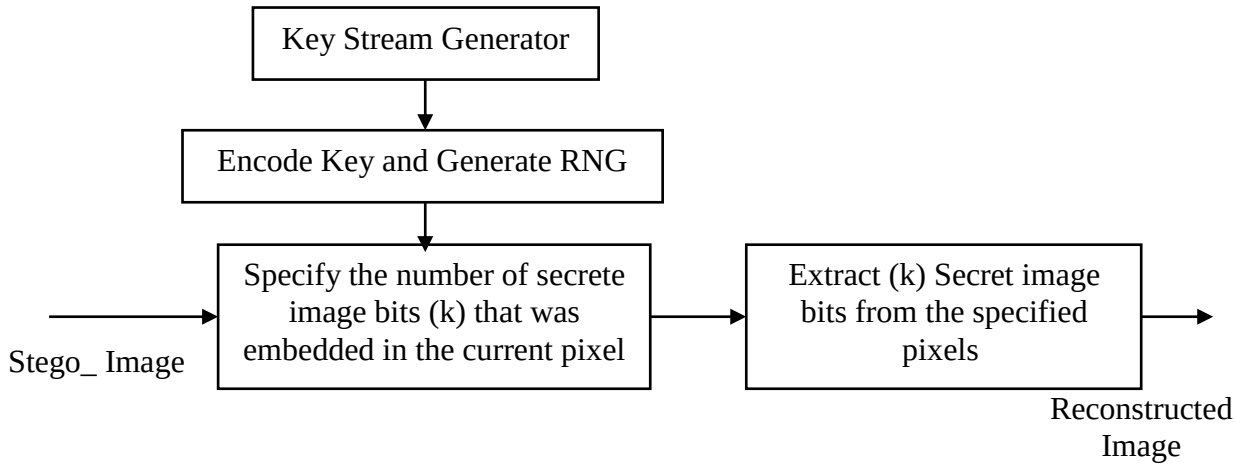


Figure ١: The Block Diagram of LFSR Key Generator



a- Embedding



b - Reconstruction

Figure 2: The block diagram of the proposed image hiding System

a- Cover Image

b- Secret Image

c- Stego_ Image

d- Reconstructed Image

Figure 3: Group1 Cover Image, Secret Image, stego_image and Reconstructed Image

a- Cover Image

b- Secret Image

c- Stego_ Image

d- Reconstructed Image

Figure 4: Group2 Cover Image , Secret Image, Stego_image and Reconstructed Image

Table 1

Group	MSE between Stego_Image And Cover Image	Correlation Between Stego_Image and Cover Image	Cover Image Energy	Stego_Image Energy	PSNR
Group 1	8.20025e-005	0.998607	0.398423	0.398868	88.992533
Group 2	9.50212e-005	0.998857	0.283966	0.286658	88.352598
Group 3	8.07074e-005	0.999032	0.303652	0.303536	89.061670
Group 4	8.03988e-005	0.999402	0.238824	0.239183	89.078307
Group 5	8.01754e-005	0.998582	0.201385	0.202082	89.090322

Table 2

Group	MSE Between Secret and Reconstructed Image	Correlation Between Secret and Reconstructed Image	Secret Image Energy	Reconstructed Image Energy
Group 1	0	1	0.420395	0.420395
Group 2	0	1	0.601370	0.601370
Group 3	0	1	0.255287	0.255287
Group 4	0	1	0.4429467	0.4429467
Group 5	0	1	0.554775	0.554775