Design and Simulation of Hiding Message Encrypted using Pseudo Random Number and Sequential Encoding

Sabah A. Gitaffa
Electrical Eng. Dep. University of Technology
Sabahahg@yahoo.com

Abstract

In this paper, a hiding encrypted message using pseudo random number generator and sequential encoding is proposed. This algorithm can provide better security of hiding information in image. The main emphasis in mine results will be on visual image quality and also the peak signal to noise ratio (PSNR) value which is a measure of quality of embedding. The results of statistical analyses like average difference, PSNR and MSE indicate high security and suitability of the proposed scheme. The obtained result shows the peak signal to noise ratio is 79dB. The programming language MATLAB is used for implementing the proposed algorithm.

Keywords: Information hiding, Pseudo-noise code generator, Sequential decoding.

1 Introduction

The worldwide data sharing offered by the advances in system interchanges has brought on a huge number of security dangers for putting away and transmission of multimedia content. So to store and/or transmit the delicate data like content, discourse and picture safely over remote/PC systems and encryption is essential, which is the primary center of the present work. In encryption, the data under thought is changed over from the understandable structure to immeasurable one and back again at the flip side, rendering it indiscernible by the meddlers without the mystery learning (secret key, encryption/unscrambling algorithm) [1]. The security of advanced image has turned out to be increasingly vital because of the fast development of the Web in the computerized world today. The security of computerized pictures has pulled in more consideration as of late, and a wide range of picture encryption techniques have been proposed to upgrade the security of these pictures. Picture encryption strategies attempt to change over a picture to another that is difficult to get it. Then again, picture decoding recovers the first picture from the encoded one. There are different picture encryption frameworks to scramble and decode information, and there is no single encryption calculation fulfills the diverse picture sorts. The majority of the calculations particularly intended to scramble computerized pictures are proposed in the mid-1990s. Pictures are not the same as content. This implies not all conventional cryptosystems are reasonable to encode pictures straightforwardly. It is not a smart thought for two reasons. One is that the picture size is quite often much more prominent than that of content. Subsequently, the customary cryptosystems require much time to specifically encode the picture information. The other issue is that the decoded content must be equivalent to the first content. In any case, this prerequisite is a bit much for picture information. Due to the nature of human eyes, an unscrambled picture containing small distortion is usually agreeable [2,3]. Unik L. and A. K. Gulve in [4] discusses the important aspects of steganography and cryptography and shows how a simple LSB steganography technique in images can be complicated further using combination of cryptography and pseudo-random number generator. A novel approach of steganography and cryptography has been developed by Gurwinder K., Navdeep S. and Sethi S. H., where an image based steganography that uses LSB techniques and pseudo random encoding technique on images to enhance the security of the communication [5]. Marwa M. E., Abdelmgeid A. A. and Fatma A. O. propses a new image steganography method based on spatial domain is proposed. According to the proposed method, the secret message is embedded randomly in the pixel location of the cover image using Pseudo random number generator (PRNG) of each pixel value of the cover image instead of embedding sequentially in the pixels of the cover image. This randomization is expected to increase the security of the system [6].

2 Pseudo-noise code generator

Pseudo random binary sequences (PRBSs), also known as pseudo noise, linear feedback shift register (LFSR) sequences or maximal length parallel successions (m sequences), are broadly utilized as a part of computerized correspondences. In a genuinely irregular grouping the bit design never rehashes. Pseudo-Noise (PN) arrangements whose terms depend in a straightforward way on their forerunners. Such successions are effortlessly created by recursive systems. PN groupings that are valuable for discourse encryption must have auto-correlation and cross-correlation properties and additionally keeping up some irregularity properties. The security offered by the framework relies upon the

haphazardness of PN arrangement. PN-arrangements created by the utilization of elliptic bends have more haphazardness and in this manner, it acts more like a commotion, thusly hard to identify. A pseudo arbitrary paired grouping is a semi-irregular succession as in it seems arbitrary inside the arrangement length, satisfying the requirements of haphazardness, yet the whole arrangement rehashes inconclusively. To a casual observer the sequence appears totally random, however to a user who is aware of the way the sequence is generated all its properties are known. PN successions have a few fascinating properties, which are misused in an assortment of uses. As a result of their great autocorrelation two comparable PN groupings can without much of a stretch be stage synchronized, notwithstanding when one of them is tainted by commotion. A PN arrangement is a perfect test signal, as it reproduces the arbitrary attributes of a computerized flag and can be effortlessly produced [3,7].

3 Hiding

Information hiding is a common, simple technique to embedding information into a file. The most used method of information hiding is a Least Significant Bit (LSB) algorithm. The LSB is the lowest significant bit in the byte value of the image pixel [8]. There are two types of LSB based on image format (8-bit, 24-bit) [9,10]. In 24-bit color image there are a 3-bits from each pixel of image can be stored to hide an image by using LSB algorithm. The information hiding based on LSB is as following steps:

- Read the 24-bit image-1 in RGB format (Red (8-bit), Green (8-bit) and blue (8-bit)),
- Preform dec2bin conversion (Decimal to Binary) for image-1,
- Read the 24-bit image-2 in gray format.
- Preform dec2bin conversion (Decimal to Binary) for image-2,
- Let the first RGB pixel of image-1 is [11011111 11000110 10000111],
- Let the first gray pixel of image-2 is [00110101],
- Perform the replacing 2 bit of LSB of each of RGB component and then hiding first 2 most significant bits (MSB) of first pixel of image-2 to RED component,
- Repeat the previous step for the second 2 MSB of first pixel of image-2 to GREEN component and lastly another next 2 MSB of first pixel of image-2 to BLUE component.
- The final result of first pixel of output image is: [11011100 11000111 100000101].

4 Sequential decoding

Sequential decoding was proposed by Wozencraft as a problematic technique for unraveling convolutional codes. The basic thought is that the decoder recovers the message grouping by speculating its way through the time-extending tree of conceivable transmitted successions. Consecutive deciphering (with infinite requirement length) works as follows. Firstly, the encoder creates its taps haphazardly and freely as portrayed previously. Consider the convolutional encoder from figure (1) and its related tree structure in figure (2). Assume we encode the message succession (1,0,0) as 111 010 100 yet get 001 010 100. Endless supply of 001 the decoder selects the most likely transmitted symbol, a 0, and heads into the tree in that bearing. It stores the expense of this move as 1, the hamming separation between the got 3 bits and the chose 3 bits. The following two got images lead it to disentangle two more zeros. These choices, unavoidable as they are given the first decision of got image, cause the decoder's expense to ascend at a strangely high rate. Eventually it realists this (contingent upon how rapidly the decoder begins second speculating itself), and chooses to turn back and attempt a different way. After it comes back to the starting and takes the upward way it has a spotless race to the end and acquires an aggregate Hamming expense of 1 for the decoded succession. All the more critically the decoder will accurately unravel the arrangement without analyzing every one of the 8 ways. The thought behind successive unraveling is that if the commotion level is little in respect to the rate of the code, the decoder can figure its way through the tree of conceivable got groupings - it need not look at each way so as to translate with diminishing likelihood of mistake. The decoder keeps a running metric intended to, overall, increment when it is going along the right way, and decline generally (in the above case the metric was simplified with the goal that it expanded rapidly along false ways and gradually along genuine ways). At every tree profundity it analyzes the metric to an adjusting limit and chooses to either push ahead, more profound into the tree, along the side to the closest branch or in reverse. In the meantime it might raise or lower its edge on the off chance that it regards it to be excessively obliging [11,12].

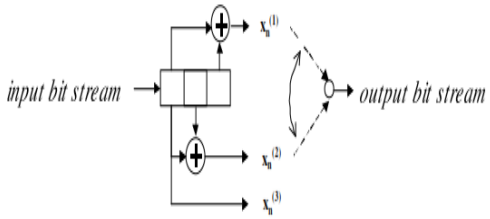


Figure 1: Convolutional encoder [10].

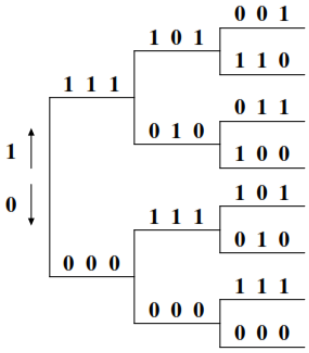


Figure 2: Decoding tree [10].

5 Proposed Methodology

This section presents the proposed algorithm with a brief introduction. The proposed method is shown in Figure 3. The method steps are shown in the following:

Input Part

- Select Image.

```
[FileName,PathName] = uigetfile({'*.Tiff';*.jpg';'*.png';'*.gif';'*.bmp'},
img = imread( strcat(PathName,FileName) );
```

- Determine Message Size

```
[hideM1,hideN1] = size(msg_temp);
hideM = num2str(hideM1);
hideN = num2str(hideN1);
dimM = length(hideM);
dimN = length(hideN);
```

Key Generation Part

- The PN sequence generator random keys depend on identification keys (Key1 and Keys 2).

```
%Generation of first m-sequence
Bit1 =[0 0 0 1 0 0 0 1];
PN1=[];
for j=1:G
PN1=[PN1 bit1(8)];

%Generation of second m-sequence
Bit2 =[0 0 0 1 0 0 0 1];
PN2=[];
for j=1:G
PN2=[PN2 bit1(8)];

KEY = bitxor (PN1(L),PN2(L));
```

Encryption Part

- Encrypting the message using XOR

```
msgenc = bitxor(uint8(msgtemphead),uint8(key));
msgencset = dec2bin(msgenc, 8);
```

Output Part

- Hiding message in image using LSB algorithm

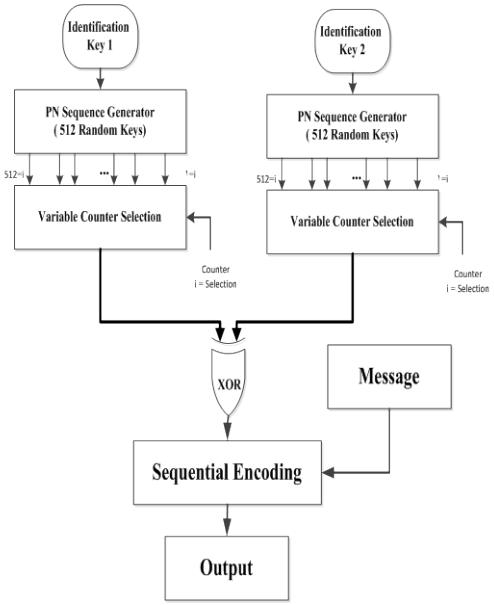


Figure 3: The structure flow of the work.

6 Simulation Results and Discussion

The proposed algorithm has been implemented in the working platform of MATLAB (version 8.1). In this paper, a 256 × 256 size image (TIFF) is used for cover image and 672 Bytes for message size. To test the performance of the proposed system, the PSNR parameter is used to evaluate the quality of image. The PSNR ratio is defined as a quality measurement between the original image and stego image. The higher of PSNR parameter improves the quality of the stego image. For wireless applications, PSNR values are between

30 db and 50 db. The PSNR is calculated by using equations (1)[13,14]:

$$PSNR_E = 10 \cdot \log_{10}\left(\frac{255^2}{MSE}\right). \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Figure 4 (a,c) shows the original image and embedded image. The PSNR value is 79 dB for stego image. While information fig 4 (b) is completely unseen and cannot be perceived by eye and quality of image remain unchanged. The final result of measurements are (MSE = 7.0190e-4, PSNR = 79.6680 dB and Average Difference 3.0518e-04). Table (1) shows the comparison of results between different techniques.

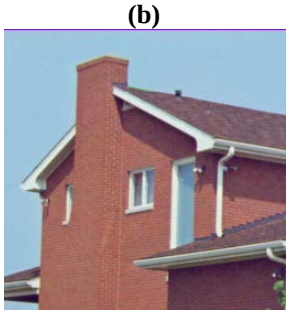
Table (1)

Parameter	Our Method	[4]	[5]	[6]
PSNR	79.6	55.6	49.3	44

(a)

The global information sharing off
has caused a multitude of security
content. In order to store and/or
speech and image securely over wir
which is the main focus of the pre
consideration is converted from th
back again at the other end, rende

(b)



(c)

Figure 4: (a) Input image, (b) message, (c) output image.

7 Conclusion

In this paper, a hiding message encrypted using pseudo random number and sequential encoding is proposed. This algorithm can provide better security to hiding information in image. The main emphasis in mine results will be on visual image quality being preserved and also the Peak SNR value which is a measure of quality of embedding. The results of statistical analyses (MSE = 7.0190e-4, PSNR = 79.6680 dB and Average Difference 3.0518e-04) indicate high security and appropriateness of the proposed plan. For future work, we can apply our algorithm on different types of sources (audio and video) to protect information for biometric applications.

References

[1] B.K. Shreyamsha Kumar and Chidamber R Patil, "JPEG Image Encryption Using Fuzzy PN Sequences", Signal, Image and Video Processing, Vol. 4, No. 4, 2010.

[2] Suhad Latef, Najwan A. Hassan and Ban N. Dhannoon, "Color Image Encryption using Random Password Seed and Linear Feed Back Shift Register", Al-Nahrain University College of Engineering Journal (NUCEJ), Vol.14 (1), March 2011.

[3] Prabir Kr. Naskar and Atal Chaudhuri, "A Secure Symmetric Image Encryption Based on Bit-wise Operation", I.J. Image, Graphics and Signal Processing (IJIGSP) Journal, Vol.6, No. 2, 2014.

[4] Unik L. and A. K. Gulve, "Steganography using Cryptography and Pseudo Random Numbers", International Journal of Computer Applications, Vol.96, No.19, 2014.

[5] Gurwinder K., Navdeep S. and Sethi S. H., "Novel LSB Approach for Steganography", International Journal of Emerging Research in Management &Technology, Vol.4, No.7, 2015.

[6] Marwa M. E., Abdelmgeid A. A. and Fatma A. O., "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 3, 2016.

[7] Nivedita Singh and etc., "Pseudo Noise Sequence Generation using Elliptic Curve for CDMA and Security Application", International Journal for Innovative Research in Science & Technology (IJIRST), Vol.1, No.11, 2015.

[8] B.S Champakamala, K. Padmini and D. K Radhika, "Least Significant Bit algorithm for image steganography", International Journal of Advance Computer Technology, Vol.3, No. 4, 2014.

[9] M. K. Meena, S. Kumar and N. Gupta, "Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity", International Journal of Soft Computing and Engineering (IJSCE), Vol.1, No.2, 2011.

[10] G. Viji and J. Balamurugan," LSB Steganography in Color and Grayscale

Images without using the Transformation", Bonfring International Journal of Advances in Image Processing, Vol. 1, Special Issue, 2011.

[11] Lenny Grokop, "Sequential Decoding: Computational Complexity and the Cuto ff Rate", University of Berkeley Report, Can be found at: https://people.eecs.berkeley.edu/~ananth/229BSpr05/Reports/LennyGrokop.pdf, 2005

[12] Wozencraft, J. M., and Reiffen, B., "Review of 'Sequential Decoding' ", IRE Transactions on Information Theory, Vol.7, No. 4, 1961.

[13] Sh. A. Laskar and K. Hemachandran,"High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS), Vol.4, No.6,2012.

[14] H. Yang, X. Sun and G. Sun,"A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Radio Engineering Journal, Vol. 18, No.4, 2009.

تصميم ومحاكاه رسالة مشفره مخفية باستخدام مولد رقم عشوائي وترميز التتابعي

المدرس صباح عبد الحسن كطافة
قسم الهندسة الكهربائية
الجامعة التكنولوجية

الخلاصة

في هذه البحث، تم اقتراح رسالة مشفره مخفية باستخدام مولد رقم عشوائي وترميز التتابعي. هذه الخوارزمية يمكن أن توفر أمان افضل في إخفاء المعلومات في صورة. التركيز الرئيسي في النتائج ستكون على جودة الصورة البصرية و أيضا على القيمة PSNR الذي هو مقياس جودة التضمين. نتائج التحليلات الإحصائية مثل متوسط مربع الخطأ ، نسبة الإشارة إلى نسبة الضوضاء و متوسط الفرق تشير إلى درجة عالية من الأمن و ملاءمة الخوارزمية المقترحة. النتائج التي حصل عليها تظهرنسبة إشارة إلى نسبة الضوضاء (PSNR) هي dB79. تم تنفيذ الخوارزمية المقترحة باستخدام لغة البرمجة MATLAB.