# Blind Color Image Steganography in Spatial Domain

**F. A. Abdullatif, W. A.Shukur**
**Department of Computer Science , College of Education Ibn Al-Hatham, University of Baghdad.**

**Received in December 19 2010**
**Accepted in Feb. 8 2011**

## Abstract

With wide spread of internet, and increase the price of information, steganography become very important to communication. Over many years used different types of digital cover to hide information as a cover channel, image from important digital cover used in steganography because widely use in internet without suspicious.

Since image is frequently compressed for storing and transmission, so steganography must counter the variations caused by loss compression algorithm.

This paper describes a robust blind image steganography, the proposed method embeds the secret message without altering the quality by spraying theme on the blocks in the high order bits in color channel such blue "without altering the human vision system" and make them integral to cover.

This method depends on constant sequence spread spectrum method and survives loss compression image like JPG.

**Keyword**: information hiding, color image steganohrapy, spread spectrum.

## Introduction

The prevalence of multimedia data in our electronic world exposes a new avenue for communication using digital steganography. Steganographic techniques are useful to convey hidden information by using various types of typically-transmitted multimedia data as cover for concealed communication. The inability to detect the hidden data, perceptually or by computer analysis, is paramount for surreptitious operation[1][2].

There are many applications for techniques that embed information within digital images.

Steganogrphy where the original cover signal is needed to reveal the hidden information are known as cover escrow. In many applications it is not practical to require the possession of the unaltered cover signal in order to extract the hidden information. More pragmatic methods, known as blind or oblivious schemes, allow direct extraction of the embedded data from the modified signal without knowledge of the original cover.

A block diagram of a blind image steganographic system is depicted in fig 1. A message is embedded in a digital image by the stegosystem encoder. The resulting stegoimage is transmitted over a channel to the receiver where it is processed by the stegosystem decoder.

During transmission the stegoimage can be monitored by unintended viewer who will notice only the transmittal of the innocuous image without discovering the existence of the hidden message.

It's known that any natural image has big amount of spatial redundancies for this reason continues tone image compression exist to remove those redundant information and represent the data in more efficient form suitable for storing and transmitting [3].

Although basic image compression stander like JPG is based on DCT, but recently new image compression stander has been proposed that is based on wavelet transform, but like any transform domain approach, DCT[4],wavelet[5]domain data hiding, demands high computational complexity that is disadvantage for real time data embedding and retrieval process.

Moreover, control on image visual quality and simple low cost hardware realization of transform domain data hiding is not always easy

Spread Spectrum Image Steganography , is a data-hiding/hidden-communication method that uses digital imagery as a cover signal. Spread Spectrum Image Steganography provides the ability to hide and recover, error free, a significant quantity of information bits within digital images, avoiding detection by an observer. Furthermore, Spread Spectrum Image Steganography is a blind scheme because the original image is not needed to extract the hidden information. The proposed recipient need only possess a key in order to reveal the hidden message[6].

## Proposed method

In this section, we will describe the blind steganography method that survives with loss compression, the main idea behind method that the joint photography expert group "jpeg" compression algorithm loss some image information, but not change the image quality.

The jpeg algorithm is a loose algorithm this will produce small amount of visual distortion, and will introduce error in the image data but this error data still nearest from original image data to avoid visual change on image because large change in data (gray scale to any color band) make visual distortion.

For that we used 24 bitmap image as a cover and embedded secret data in spatial domain in 8*8 block in one channel values and leaving the other channel unchanged then the stego image is store in jpeg format

In this method we use a table of 256 entries and divide the table to several period, all periods are the same length as in table 1 and each center of period take 0 and 1 respectively.

In the embedding process, each block 8*8 from cover image used to embedded one secret bit by adjusting the value of cover image data to center of period closed to secret bit, the period and center of period as in table 1 stego table, example to explain embedded process, let the secret bit is 0 and the value of blue channel is 25 "we use blue channel to embedded because human vision system HVS is less sensitive to blue change than the red or green " we change the 25 to the nearest periods that have 0 "secret bit in example" in center these periods 32 -47 or 0-15 the center of the first is 39 and the difference is 14 and the center of the second period is 7 and the difference is 18, then change the value to 39 because had less difference "we use this two periods because the secret bit 0 and the value of the blue channel is 25 and the nearest periods have 0 in center these period".

Each pixel "channel values "have two periods or more depend on secret bits except the boundaries value near 0 or near 255 have only one adjust value and not need to compute and compare process.

This process will repeat for all 8*8 blocks, in the worth case the change not exceeded the distortion caused by jepg algorithm.

After receiving stego image we assembly the 8*8 blocks in blue channel and read the value to know the period value and then the secret bits.

Extra method will use to overcome the high distortion in some pixel value that can appear in jpeg algorithm "like noise and rapidly large change in value" that the extracting come from block 8*8 then can measure the entropy of 0 and 1"number of 0 and 1 in block " and if the entropy of 0 more than, the secret bit in block is 0 or if entropy of 1 larger, then the secret bit is 1, my experimental test show that no block have the same entropy to 0 and 1

## The purpose of use 16 as interval length

We use 16 as period length this make the change in value less than the HVS sensitive and be normal with the distortion of jpeg algorithm and also large to overcome the error counter in jpeg compression, and also to avoid producing pattern can use in attack where the output 16 numbers and after compress can be any number from 256 numbers.

**The proposed embedded algorithm**

1- Split the cover image to three arrays RGB "we use a true color 24bit image"

2- Take the blue array and use the first 8*8 block to store o if secret message is text or 1 if secret message is a file.

2- if stego message is text then take next 8*8 block to store 0 for Arabic and 1 for English then use encode decode table that use 6 bits to encode the letter with 64 different symbol "if second 8*8 block have 0 then take Arabic letter with special char table or if 1 then take English letter with special char table and the output is binary array

Or if stego message is a file encode the file to binary array

3- Compute if the cover file can store all stego message or not

$$Size_{st} = (length*high) / 64 + i*64$$

- Where i =2 if used text message and i =1 if used file

If binary message array is more than $Size_{st}$ then suggest to replace the cover image with other image have larger dimension and return to 1

5-Repeat until all secret bits are embedded

i-read secret bit

ii-for each 8*8 block:- read the data of block and change it to the nearest period center depend on table 1 and process compute and compare" compute difference and compare to choose less difference"

6- Put end of message sign if the text message is used, use EOF sign if a file used

**Arabic-English encode and decode table**

This table contains two fields and 64 records one field for char and other for 6 bits binary code representing char and the last record in Arabic and English table is useded to the end message sign

In embedded process compare the char with first field and put the corresponding binary in second field to binary array

In the extracting process check the binary with the second field and take the corresponding char in the first field

We use this table for more security through encode each char in binary code different in asscii and for more space through each letter takes 6 bits rather than 8.

# Extracting

In extracting we read the first block and know the embedded message either text or file and if text read the second block to know decode in Arabic or English table then read each block and after reading the value of each block items determine the period then the secret bit from table1 after computing the entropy of 0 and 1 in block, until reaching to the sign of end message in text or EOF sign in file, example if the first item in block have 178 then it is in 176-191 period and the secret bit is 1

**Experimental result**

We have tested the proposed embedding method with many images and show in low frequency area "smooth area" that have approximate identical pixels values the number of distortion "error" in jpeg algorithm is less than the other area "high frequency area "for that we can use block smaller than 8*8 block in this type of area to embedd the secret bits and recover with error free secret message.

For more robust we use multi periods to make the distributed for all image value range and the pattern from the move image cover value to the center of period can alter in the compression process and the value of distortion from compression process is different and within the range of normal compression as shown in fig 2 the two images used as cover and fig 3,4 the histograms to each bands RGB of the two images in fig 2 respectively before compress, fig5 the two images after hiding information and compress and receive the other side, fig 6,7 the two images histograms of fig 5, we can notice that the distortion of the blue channel that is used to hide information approximately same in red R and green G where the R and G that not changed only the distortion of compression happen on it.

We can also use two or three bands for embedding process with low compression value "approximately less 60"

Also we can use block 4*4 if the compression value less than 55

# Conclusion

In this paper, we have proposed new robust blind steganography methods by this method store secret message in one band "use blue band" in 8*8 blocks and can survive with

jpeg compression and any DCT base compression without sensitive of HVS and still have the same statistical property.

## References

1. Bender, W.; Gruhl, D.; Morimoto, N. and Lu, A.(1996) , Techniques for data hiding .IBM system journal,35(3-4).

2. Cox, I. J.; Kilian, J. and Shamoon, T. September (1996), secure spread spectrum watermarking for images, audio and video. Proceeding of IEEE international conference on image processing, Lausanne,Switzerland,III:243-246

3. Fridrich, (1998) , Application of data hiding in digital image ,URL:http://www.ssie.binghamton.edu/~jirif

4. Riley Mary, J. and Richardson Iain, E.G.( 2007), Digital image and Video Communications, ArtechHouse, Bosten,London.

5. Tsai, C.S., C. C, T. S., Chen ,( 2006), Sharing multiple secrets in digital images, the journal of systems and software.

6. Avcibas, I. Memon, N. and Sankur ,B.(2008), steganalysis using image quality metrics, Wiley-interscience .

**Table: (1) The stegano table**

| 0-15 | 16-31 | 32-47 | 48-63 | 64-79 | 80-95 | 96-111 | 112-127 | 128-143 | 144-159 | 160-175 | 176-191 | 192-207 | 208-223 | 224-239 | 240-255 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 23 | 39 | 55 | 71 | 87 | 103 | 119 | 135 | 151 | 167 | 183 | 199 | 215 | 231 | 247 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

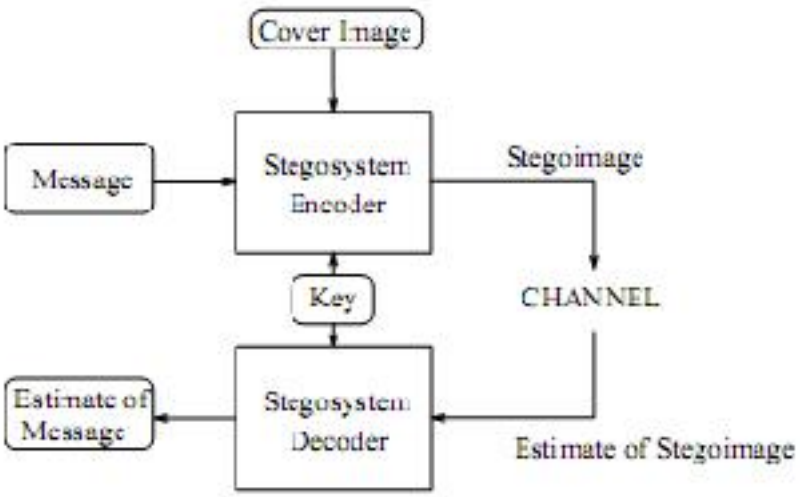
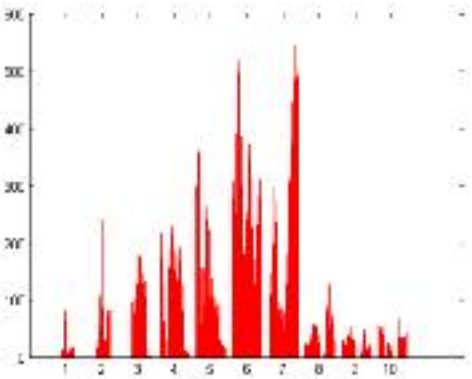



**Fig. (1): a blind image steganographic system**

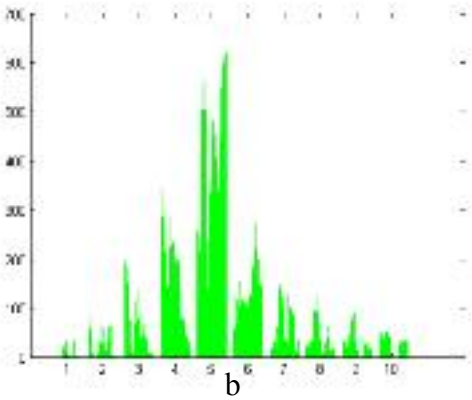
a

b

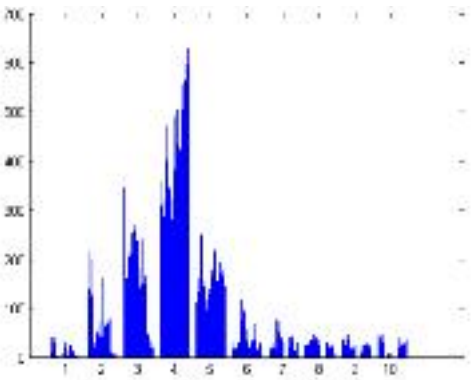
**Fig.( 2): a and b is a BMP image used as cover image**



a

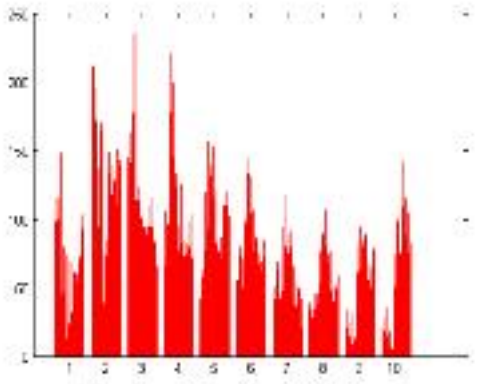


b

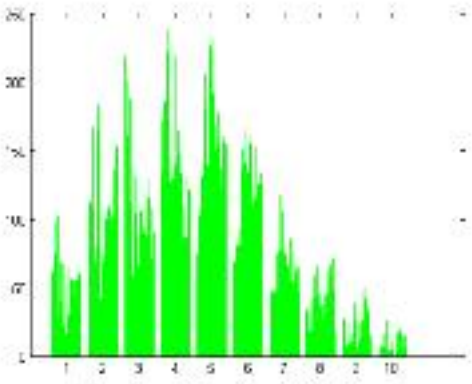


c

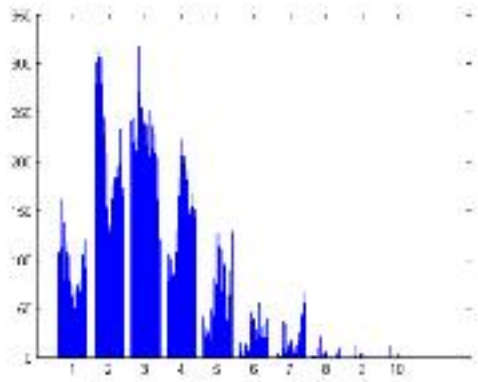
**Fig.( 3): a – red band histogram, b- green Band histogram and c- blue band Histogram for fig 2 a**



a



b



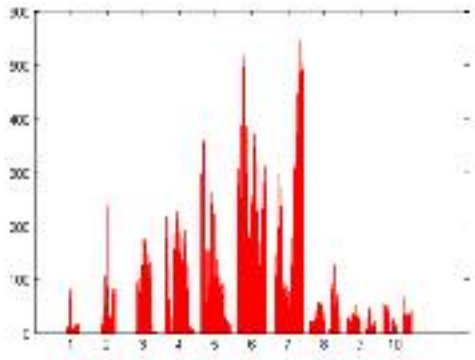
c

**Fig.( 4): a – red band histogram, b- green Band histogram and c- blue band Histogram for fig 2 b**

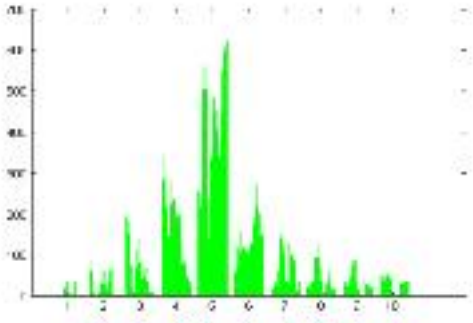
a

b

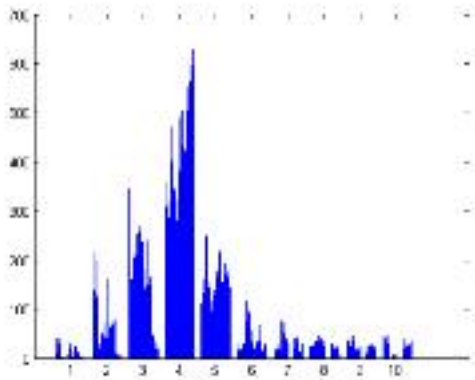
**Fig.( 5): a is the same of fig 2 a in the receiver side and b is the same of fig 2 b in the receiver side that use to extract message**



a

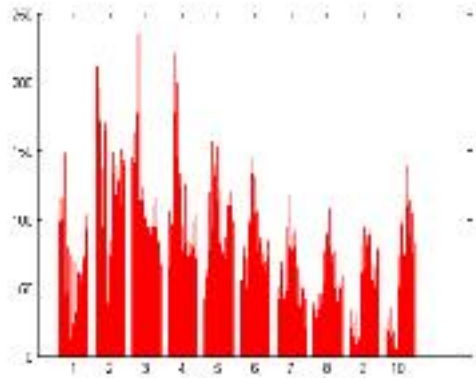


b

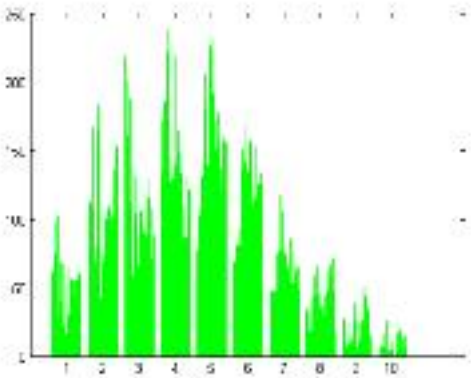


c

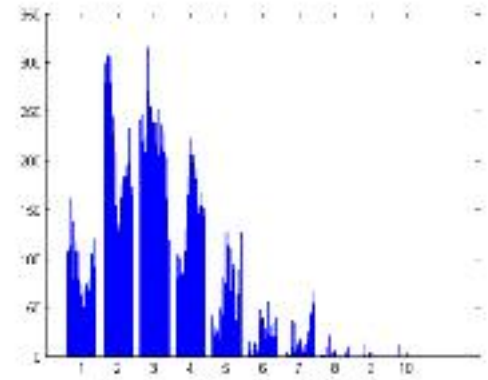
**Fig.( 6): a – red band histogram, b- green Band histogram and c- blue band Histogram for fig 5a**



a



b



c

**Fig. (7 )a – red band histogram, b- green and histogram and c- blue band Histogram for fig 5 b**

مجلة ابن الهيثم للعلوم الصرفة والتطبيقية المجلد24 (1) 2011

# طريقة عمياء لإخفاء بيانات داخل صورة ملونة في مجال الصورة

**فراس عبد الحميد عبد اللطيف ، وسام عبد شكر**
**قسم علوم الحاسبات ، كلية التربية– ابن الهيثم ، جامعة بغداد**

**استلم البحث في 19 كانون الاول 2010**
**قبل البحث في 8 شباط 2011**

## الخلاصة

مع الانتشار الواسع للانترنت والزيادة الكبيرة في قيمة المعلومات، أصبح نقل البيانات المخفية أمرا" مهما" جدا.

على مر السنين استعملت أنواع مختلفة من الأغطية الرقمية لإخفاء المعلومات وإرسالها في قنوات مخفية، تعد الصورة من أهم هذه الأغطية الرقمية لانتشارها الكبير في الانترنت وإمكانية تداولها من دون أي شكوك.

بما إن الصورة تضغط عادة للخزن والنقل لهذا يجب أن تكون طرائق أخفاء البيانات قادرة على الاحتفاظ بالبيانات مع هذا الضغط.

يوصف هذا البحث طريقة جيدة لإخفاء البيانات في صورة ، اذ ان الطريقة المقترحة تخفي النص السري من دون تغير بنوعية بيانات الصورة وذلك برش النص على مجموعة من الكتل" البلوكات" في قناة من قنوات الصورة، مثل قناة اللون الأزرق ومن دون تغيير في الصورة ممايجعل الرسالة السرية متكاملة مع خصائص الصورة

تعتمد هذه الطريقة على طريقة نشر السلسلة الطيفية الثابتة وتبقى الرسالة المخفية صحيحة حتى بعد الضغط مع الفقدان"ضغط الخسارة"