Implementation Suggested Method For Steganography

Hiba Mohammed Ja'fer
Babylon University, College of Computer Technology, Dept of Information Networks

Abstract

Steganography is an ancient art or conveying messages in a secret way that only the receiver knows the existence of a message. In this paper, a novel mechanism using mathematical modulus to incorporate the secret data (with audio form) into a cover-image .The modulus is a threshold value that determines how the embedded file is incorporated into the cover-image. The proposed method aims to meet most the requirements of any steganography system (like capacity, security and undetectability),we compress the embedded file in order to reduce the size of it and increase the security .Furthermore, the quality of stego-image measured by PSNR is acceptable to human vision system and stable for diverse cover-image processes.

الخلاصة

تعاني معظم طرائق إخفاء المعلومات من عدة مشاكل تؤثر على كفاءتها وأدائها. وبعض هذه المشاكل هي سعة الوسط الغطاء وتشويهه، الخ. اقترحنا في هذا البحث طريقة جديدة لإخفاء ملف صوت (بهيئة WAV) في ملف صورة (بهيئة BMP) تتجاوز معظم تلك المشاكل. كما تحاول تلبية متطلبات أي نظام اخفاء مثل (السعة، السرية وعدم القدرة على الاكتشاف). وهي تعتمد على استعمال الاسلوب الرياضي لدمج البيانات السرية (الصوت بعد ضغطة باستخدام خوارزمية DCT) مع صورة الغطاء.وتُعدُّ هذه الطريقة ذات أمنية عالية لأنّ البيانات السرية تضاف إلى صورة الغطاء .و إنّ البيانات المخفية لن تسترجع إلا بمعرفة خوارزمية الإخفاء .وفي حالة معرفة خوارزمية الاسترجاع فإنّ الصورة المخفية لن تسترجع إلا بعد فك الضغط ،إضافة إلى معرفة المعلومات السرية المشتركة بين المرسل والمستلم وهي بذرة مولد الأرقام شبه العشوائية (**Sk**)،متسلسلة الأعداد (**S**)،وعدد الثنائيات المخفية(m_l,m_u) وقيمة العتبة (**T**).كذلك استعمال الاسلوب العشوائي يجعل عملية الوصول إلى الصورة المخفية صعبة.

1-Introduction

Steganography is a means of storing information in a way that hides information's existence. Steganography contains the techniques for secret hiding of messages in another wise innocent looking carrier message. The purpose of steganography is not to keep others from knowing the hidden information, but is to keep others from thinking that the information even exists (D.Artz)(2004). Therefore, the main goal is to not raise suspicion and avoid introducing statistically detectable modifications into the carrier media(S.Lyu and H.Farid)(2006),(J.A.Memon ,K.Khowaja and H.Kazi)(2008),(S.Katzenbeisser and F.A.P.Petitolas)(2002).

Historically, the first steganography techniques included invisible writing using special inks or chemical(D.Kahn)(1996). Today, it seems natural to use digital images, digital video or audio for hiding secret message(J.Fridrich)(1998). Steganography, like watermarking and fingerprinting, is a branch of information hiding. Unlike watermarking and fingerprinting, steganography imposes the requirement that the presence of a hidden message within the stegotext (transmitted data) should be undetectable (P.Moulin and Y.Wang)(2004). One of the most common uses of modern steganography in digital world of computers is to hide information from one file in the contents of another file (K.Rabah)(2004),(M.A.B.Younis and A.Janta)(2008) .

Most steganography methods suffer from many problems (or impose constraints), make the results of its failure against steganalysis. One of the limitations

of steganography is the one-to-one relationship between an embedded and cover file (E.Cole)(2003): to hide one byte of covert data requires one byte of overt data. The amount of data that can be effectively hidden in a given medium tends to be restricted by the size of the medium itself (D.Artz)(2001). The common well-known steganographic method is the least significant bits (LSBs) substitution (C.C.Chang and H.W.Tseng)(2004). Many public steganographical software , such as S-Tools , EZstego and Steganos apply this method(X.Luo,F.Liu and P.Lu)(2007). In this method there is a limit for the number of substituted bits (N.Cvejic and T.Seppanen)(2004)(the maximum depth of LSB insertion is 4-LSB (Y.K.Lee and L.H.Chen)(2000).

Images are a good media for hiding data and have the lenient constraints (D.Artz)(2001). This media have many problems when it used in steganography as a cover. One common drawback of virtually current data embedding methods is the fact that the original image is inevitably distorted by some small amount of noise due to data embedding itself (M.Goljan,J.Fridrich and D.Rui)(2001). Another problem, we did not have to change all of the LSB's (underlined), which means that on average 50% of the pixels of an image will not be affected by embedding (the embedding capacity is 50% of the cover-image size). The problem above appear when LSB's insertion is used (K.Rabah)(2004),(Y.K.Lee and L.H.Chen)(2000). Third, is that the limitation on the available colors imposed by the finite palette makes the process of message hiding a difficult challenge (the order of the palette will change after embedding) (J.Fridrich)(1998).

This paper has been attempted to solve these problems and aim to satisfy the requirements of steganography system (capacity, security and indefectibility). A new, simple, and secure method has been proposed which transferring the secret message (audio file) after compressed (using DCT) into bit-string and find the workable pixel in cover image by using pseudo-random number generator of seed to create less distortion stego-media to meet the main goal of steganography . Also the capacity evaluation is provided to estimate the maximum embedding capacity of each pixel,to maximize the capacity of cover media and simplifying the limits on the size of secret massage. So the method based on compressed file rather than the file itself and this give additional secure level for message .

The rest of this paper is organized as follows. The new scheme is presented in Section 2. Implementation results are in Section 3. Conclusions are drawn in Section 4.

2-The proposed algorithm

Most researches are concerned on the LSB method for data hiding. This method, as explain previously, have many problems that effect on the performance of the embedding method. For this and to get a secure embedding, we proposed a new method that hiding audio file with WAV format in a BMP image file by using a mathematical modulus to incorporate the secrete audio into a cover image . It's overcome LSB's problems and aiming to satisfy most the requirements of steganography system, especially the two main aspects (security and capacity), that affecting on the steganography and its usefulness.

First, the algorithm starts with dividing the data of audio file U(M) with m=1,…,M into blocks with size (8×8) bytes for each and perform a two-dimentional (DCT) .

$$DCT(u,v)=\alpha(u)\alpha(v)\sum_{i=0}^{N-1}\sum_{i=0}^{N-1}U(r,c)\cos\left[\frac{(2r+1)u\lambda}{2N}\right]\cos\left[\frac{(2c+1)v\lambda}{2N}\right]$$

$$\alpha(u),\alpha(v)=\begin{cases}\sqrt{\frac{1}{N}} & for\ u,v=0\\ \sqrt{\frac{2}{N}} & for\ u,v=1,2,..N-1\end{cases}$$

After the DCT stage we have an 8*8 matrix of real numbers . To compress we discard some of the less important information by using standard tables , which is called quantization .The next stage is the coding stage ,we using the RLE to coded the matrix[16] .

After that the coding matrix transfer into a bit-string in order to embed by using modulo mechanism[17]. Assume that the color of one pixcl *p* at co-ordinates **(x,** *y)* is denoted by f(x, *y),* the eight-neighbors of p . For *p*, f (x **,** y) will be modified according to its embedding capacity, which depends on its color and the color variation of the upper and left neighbors.The advantage of using the upper and left neighbors to estimate the embedding capacity is that when or after the current pixel is processed, the colors of these upper and left neighbors will be never changed. Therefore the embedding module and extracting module arc synchronous when estimating the embedding capacity of each pixel[18]. Let

Max(x,y) =max {f(x- 1,y- 1) , f (x - 1 , y) ,
f(x- l , y + I),.f(x,y- 1) }
Min(x,y) = min{f(x - 1 ,y - l),.f(x - 1, y)),
f(x- l , y + I),f(x,y- 1) }
D(x,y) = Max(x, y) - Min(x, y)

Except for the boundary pixels in an image, the embedding capacity Kn(x, y) of cach pixel (x, y) is defined as

$$Kn(x.\ y)=\log_2\lfloor D(x,y)\rfloor$$

The embedding capacity should be limited by the grey scale of current pixel. Here, an upper bound for embedding capacity at pixel (x, *y)* is defined as

$$U(x,y)=\begin{cases}4 & ,if\ f(x,y\le t\\ 5, & otherwise\end{cases}$$

The next scheme describe the embedding algorithm:

Embedding Algorithm

Input : The cover-image and the embedding audio message ,the seed key and two modulus numbers m_u , m_l.
Output :The stego-image and secret key.

Step1: Find the workable pixel p_c (i) in cover image C by using the pseudo-random number generator of seed sk .
Step2: Compressed the embedded-audio
-Split embedded-audio into blocks with size (8*8).
-Perform DCT Transform .
-Applied quantization .
-Coded the quantized matrix.

-Transfer the coding matrix into bit-string B_s

Step 3:Set a threshold value T and the two modulus values m_l ,m_u. then compute a residue , $g_{remainder}$ and the possible capacity in a pixel , g_{ec} , as following form:

if $p_c(i) > T$, compute $g_{ec} = \lfloor Log_2^{m_u} \rfloor$, $g_{remaimder} = p_c(i) \bmod m_u$

else , compute $g_{ec} = \lfloor Log_2^{ml} \rfloor$, $g_{remaimder} = p_c(i) \bmod m_l$

where $p_c(i)$ denotes the intensity of the i-th. pixel with order of top-down and left to-right in a cover-image C and $\lfloor \ \rfloor$ denotes the truncate value.

Step 3:Compute the absolute difference value, g_{dv}, such that

$g_{dv=} |g_{remainder} - g_{ev}|$

where g_{ev} is a value, which is fetched sequentially from Bs with bits of g_{ec} -length.

Step 4:Embed g_{dv} into the pixel $p_c(i)$ (here, we define $p_s(i)$ as the intensity of the i-th pixel after embedding g_{ev})by performing the following process:

Case I: $p_c(i) < T$

1. if $p_c(i) < \frac{m_l}{2}$, gain $p_s(i) = 0 + g_{ev}$.

2. $\frac{m_l}{2} < p_c(i) < T - \frac{m_l}{2}$

. if $g_{dv} > \frac{m_l}{2}$, gain an adaptable value, $Av = m_l - g_{dv}$.

. if $g_{remainder} > g_{ev}$, gain $p_s(i) = p_c(i) + Av$.

else , gain $p_s(i) = p_c(i) - Av$.

. if $g_{dv} \le \frac{m_l}{2}$, gain $Av = g_{dv}$

. if $g_{remainder} > g_{ev}$, gain $p_s(i) = p_c(i) - Av$.

3. If $(T-\frac{m_l}{2}) \le p_c(i) < T$, *gain* $p_s(i) = p_c(i) - g_{remainder} + g_{ev}$

Case II : $p_c(i) \ge T$

1. If $p_c(i) > (255-\frac{m_u}{2})$, gain $p_s(i)=(255-m_u+1)+g_{ev}$

2. If $(T+\frac{m_u}{2}) < p_c(i) \le 255-\frac{m_u}{2}+1)$

. If $g_{dv} > \frac{m_u}{2}$, gain $Av=m_u-g_{dv}$

If $g_{remainder} > g_{ev}$,gain $p_s(i)=p_c(i)+Av$

else ,gain $p_s(i)=p_c(i)-Av$

. If $g_{dv} \le \frac{m_u}{2}$, gain $Av=g_{dv}$

If $g_{remainder} > g_{ev}$,gain $p_s(i)=p(i)_c$-Av
else ,gain $p_s(i)=p_c(i)$+Av

3. If $T \le p_c(i) < (T + \frac{m_u}{2}), gain\ p_s(i) = p_c(i) - g_{remainder} + g_{ev}$

Step 5:Hide the embedded-header in fourth column of the stego-image palette "ps (i)".
Step 6:End.

For the header part of audio file, it is embedded in the forth column of color table (palette table) of stego-image. This part of color table provides 256 free bytes.

In the stage of extraction, every bits of audio is extracted from the stego-image depending on the positions that stored using random number generated by seed key and two modulus numbers m_u , m_l additional the receiver must know the embedding algorithm and then decompress the extracted bits . The receiver cannot able to extract the embedded-image without know the embedded positions, therefore this method is more secure. The next scheme describe the extracting algorithm :

Extracting Algorithm

Input: The stego-image, the seed key and two modulus numbers m_u , m_l. .
Output: The embedded-audio

.
Step1: Extract the embedded header of audio from palette table of the stego-image.
Step 1:Find a workable pixel p_s (i) in stego-image s by using the Pseudo-random number generator of seed Sk.
Step 2:Compute the embedded information as following
Case I:$p_s(i)<T$:

$$g_{remaimder} = p_s(i) \bmod m_l$$
$$g_{ec} = \lfloor \mathrm{Log}_2^{m_l} \rfloor$$

Case II: $p_s(i) \ge T$:

$$g_{remaimder} = p_s(i) \bmod m_u$$
$$g_{ec} = \lfloor \mathrm{Log}_2^{m_u} \rfloor$$

Step 3:Translate the $g_{remainder}$ into the bits representation to recover the embedded information ,the bit-length for each $g_{remainder}$ is determined by the computation of g_{ec} .
Step 4:Decompress the embedded information
- Decoding the embedded information
- Dequantized the decoding information
- Perform inverse DCT transform

Step 4:Recover the embedded-header from fourth column of stego-image palette.
Step 5:End.

3-The results

To stand on the performance of the proposed method, two different audio files with different sizes are applied. Also, we are used color images with 8 bits/pixel. The method emphases in selecting the audio files that its sizes larger than the image files in all experiments in order to explain how the proposed method have high-capacity

feature. We are used subject and object criteria as measures of stego-image and restored message quality. In object criteria, the following formulas are used :

i) Root mean square error (**RMSE**[*]).

$$RMSE = \sqrt{\frac{\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c) - I(r,c)\right]^2}{(M \times N)}} \quad ,(2)$$

ii) Peak signal to noise ratio (**PSNR**[*]): Here we are used two different formulas, one for images as following:

$$PSNR = 10 \log_{10} \frac{(L-1)^2}{\frac{1}{M \times N}\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c) - I(r,c)\right]^2} \quad ,(3)$$

where L represent the number of gray levels, $\hat{I}$ is the stego-image, and I is cover-image with size (MxN). Whereas, for measuring the quality of restored audio, the following PSNR[**] formula is used:

$$PSNR = 10\log_{10} \frac{\sum_{n} x^2(n)}{\sum_{n}\left[x(n) - y(n)\right]^2} \quad ,(4)$$

where x(n) represent sample of embedded audio sequence and y(n) stand for sample of restored audio sequence.

3-1: Satisfying the requirements of capacity, and undetectability.

In this experiment we attempt to embed an audio message its size larger than the cover image. The modulus values m_u,m_l are set of 32 and 16 respectively. In a sense the modulus 32 is set to accommodate the embedding of 5-bit pattern at the situation that the pixel of embedded image is greater than the threshold value T picked in our algorithm is empirically set the intensity value of 160.On the ether hand , the modulus 16 is set to accommodate the embedding of 4-bit pattern at the condition that the pixel of embedded image is less than T.

We have been tested the proposed method on a number of color images (**8 bits/pixel**) with size (**128x128**), to embed an audio message its size (**17.8 KB**). The embedding capacity approximate restored audio message are given in table (1).

It can be seen from table 1 that the proposed algorithm with generally higher **PSNR** values for restored audio message. This indicates that the restored audio file is semi to the origin. Here we don't substituted the similar blocks in order to make the stego-image without distortion.

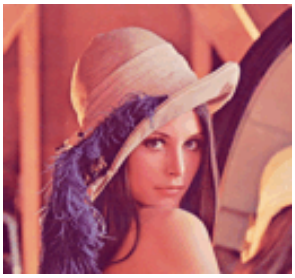
Also, the table 2 shows the results of **RMSE** and **PSNR** between the cover-images and stego-images.In such case, the embedding message is totally incorporated into cover-image. This indicates that all images less distortion, and the attacker (steganalysis) can't easily detects the embedded message. This makes the mission of the attacker is more difficult. The **RMSE** and **PSNR** values for stego-images it's acceptable and the distortions are imperceptibility to human vision. It means such distortions will be less noticeable from the viewpoint of attacker.

Table 1: The results of RMSE and PSNR for the restored audio massage.

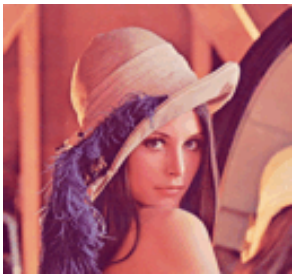
Image	RMSE (audio)	PSNR (audio)
lenna	0.037	123.248
Garden	0.02	144.341
fish	0.053	101.497

Table 2: The results of RMSE and PSNR for the stego-images

Image	RMSE(image)	PSNR(image)
lenna	0.01	95.504
Garden	0.012	87.971
Fish	0.014	80.493

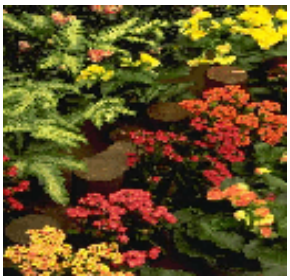


(a)

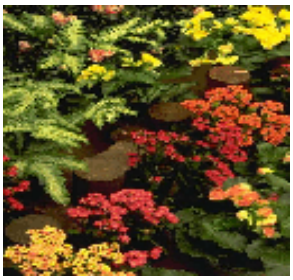


(b)

Figure (1): Lenna image (a) cover-image, (b) stego-image



(a)



(b)

Figure (2): Garden image (a) cover-image, (b) stego-image

(a)

(b)

Figure (3): Fish image (a) cover-image, (b) stego-image

4-Conclusions

This paper emphases on applying most the requirements of any success steganography system like (capacity, invisibility, security, and undetectability) and advanced the relation of one to one.

The process of compression give as the ability to hide data its size larger than the cover data. Thus, we can hide a message its size larger than the size of cover-media and make the size of message less limited in some size. At this point, here is the powerful of the proposed method by increasing the capacity of cover-media and reducing the limits of size that facing most data hiding techniques. We find from experiments that the increased size of message have no much effects on the quality of stego-image and still imperceptible. Additionally ,the compression process add another layer of protection for secrete message .

Also, when the embedding stage is completed, the stego-image less distortion or distortion-free depending on the values of **RMSE** and **PSNR** as we see in tables (1,2), respectively. This is because the changes in the values of data of cover-image is not found or not perceptual and the quality of stego-image still good . These results will reflect on the ability of human visual system. This point will reflect on the steganalysis, and makes the process of analyzing the produced steganography very difficult.

For the security requirement, the algorithm produces a sequence of secret key that send independently to increase the difficulty of steganalysis on these stego-images. The receiver can extract the embedded message by using that secret key only.

References

Artz D.,2001, Digital Steganography :Hiding Data within Data. IEEE INTERNET COMPUTING, Vol. 5, No. 3, pp. 75-80.

Lyu S. and H. Farid. Steganalysis,2006,Using Higher-Order Image Statistics. IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, pp. 111-119.

Memon, J.A. K. Khowaja and H. Kazi,2008, Evaluation of Steganography for URDU/ARABIC Text. Journal of Theoretical and Applied Information Technology, Vol. 4, No. 3.

Katzenbeisser S and F. A. P. Petitcolas.2002, Defining Security in Steganographic Systems. Proceedings of Electronic Imaging , Security and Watermarking of Multimedia Contents, Vol. 4675, pp. 50-56, San Jose, CA, USA .

Kahn, D. 1996, The history of steganography. Proceedings of the first Workshop on Information Hiding, Lecture Notes In Computer Science, Vol. 1174, pp. 1-5, 30 May 1 June, Cambridge, UK.

Fridrich J.,1998, A New Steganographic Method for Palette–Based Images. Proceedings of the IS&TPICS conference, pp. 285-289, April, Savannah, Georgia. P.Moulin and Y. Wan,g,2004 New Results on Steganographic Capacity. Proc.

Conference on Information sciences and systems, pp. 813-818, Princeton, NJ.

Rabah K.,2004, Steganography –The Art of Hiding Data. Information Technology Journal 3(3), pp. 245-269 .

Younis M. A. B. and A. Janta,2008, A New Steganography Approach for Image

Encryption Exchange by Using the Least Significant Bit Insertion. International Journal of computer science and network security, vol.8, no.6.

Cole,2003, E. HIDING IN PLAIN SIGHT: Steganography and the Art of Covert Communication. Wiley Publishing, Inc. USA.

Chang C.C. and H.W. Tseng,2004, A steganographic method for digital images using

side match. Pattern Recognition Letters, Vol. 25, pp. 1431-1437.

Luo, X. F. Liu and P. Lu.2007,,A LSB STEGANOGRAPHY APPROACH AGAINST PIXELS SAMPLE PAIRS STEGANALYSIS. International Journal of Innovative Computing, Information and Control, Vol. 3, No. 3, pp. 575-588.

Cvejic N. and T. Seppanen,2004, Increasing Robustness of LSB Audio steganography using a Novel Embedding Method. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

Lee Y. K and L. H. Chen,2000, High capacity image steganography model. IEEE Proceedings on Vision, Image and Signal Processing, 147(3), pp. 288-294.

Goljan M., J. Fridrich and D. Rui.,2001,Distortion-Free Data Embedding for Images.

Proceedings of the 4th International Workshop on Information Hiding, LNCS, Vol. 2137, pp. 27-41, London, UK.

Umbaugh S . E , 1998,Computer Vision and Image Processing , Pretice Hall , London Wang S and K.Yang 2001,AScheme of High Capacity Embedding On Image Data

using Modulo Mechanism ,WISA,Souel,Korea,

Lee Y.K and L.H.Chen,2000,high Capacity Image Sreganographic Model ,IEE

proceeding Vision ,Image and Signal Proceeding ,147,3,288 .