A New Algorithm To Hide Text Watermarking In Image

Assistant Lecture
Orooba Ismail Ibrahim

Al-Nahrain University-College of Medicine

Abstract

Watermarking has been proposed as a method to enhance data security, confidentiality and integrity. Text watermarking requires extreme care when embedding additional data within the images because the additional information must not affect the image quality.

In this paper we present a watermarking scheme that hide watermarking in method, not affect the image quality.

In this work we use Small text as a watermark to embed in images is published on the website to maintain ownership of the images for my site.

We use LSB method in hiding operation by special techniques depend on convert text watermarking to ASCII code then to binary code every character in text watermarking take 1 byte (8 bit)every three characters take three byte (24 bit)

Every three byte from text watermarking compare with pixel in palette of image , if find pixel equal with three byte of watermarking as soon as save the location of pixel .

After comparison all characters of text watermarking and find Is equivalent to from pixels in palette and save its locations in specific method in LSB of Image.

After hiding watermarking, we published the image in website that related e

Keywords: Image, web site, Text Watermarking, LSB Method, Information Hiding

الخلاصة

العلامة المائية اقترحت كطريقة لتعزيز امنية البيانات وسريتها ونزاهتها, العلامة المائية النصية تتطلب اقصى درجات الحذر عند اخفاءها كمعلومات اضافية في صورة رقمية لان المعلومات الاضافية يجب ان لا توثر في جودة الصورة .

في هذا البحث نحن نقدم نظام علامة مائية يخفي العلامة المائية بطريقة لاتؤثر على جودة الصورة.

في هذا العمل نحن استخدمنا نص صغير كعلامة مائية يخفى في الصورة المنشورة في الموقع الالكتروني للحفاظ على ملكية الصور الخاصة بموقعي .

نحن استخدمنا طريقة البتات الاقل اهمية لكن بطريقة جديدة تعتمد على تحويل النص المستخدم كعلامة مائية الى الاسكي كود ثم الى النظام الثنائي كل رمز بالعلامة المائية يأخذ 1 بايت (8 بت) , كل ثلاث رموز في العلامة المائية النصية تأخذ 3 بايت (24 بت).

كل ثلاث رموز من العلامة المائية النصية تقارن مع نقاط في بلت الصورة اذا وجدنا النقطة المناسبة نخزن موقعها .

بعد مقارنة كل رموز العلامة المائية وايجاد ما يكافئها في بلت الصورة من نقاط وخزن مواقع النقاط نخفي مواقع النقاط بطريقة معينة في البتات الاقل اهمية في الصورة .

بعد اخفاء العلامة المائية في الصورة نقوم بنشر الصورة في موقعنا .

1-**Introduction**

One of the most important properties of (digital) information is that it is in principle very easy to produce and distribute unlimited number of its copies [1].

This might undermine the music, film, book and software industries and therefore it brings a variety of important problems concerning the protection of the intellectual and production rights that badly need to be solved [9].

The fact that an unlimited number of perfect copies of text, audio and video data can be illegally produced and distributed requires studying ways of embedding copyright information and serial numbers in audio and video data, therefore using watermarking to save owner digital information .

Text watermarking is a special mark which enable you write words on your picture to protect your copy.

In recent years watermarking has become an important research area in data security, confidentiality and image integrity [3].

The proposed system using new technique to hide watermarking in image, most of the previous system hide watermarking direct in image.

The proposed system hide text watermarking indirect method , we explain these later.

2. Watermarking

Steganography and watermarking are main parts of the fast developing area of **information hiding**[6].

Steganography and watermarking bring a variety of very important techniques how to hide important information in an undetectable and/or irremovable way in audio and video data [4].

The watermarking is a method to achieve the copyright protection of multimedia contents. Because the multimedia represents several different media such as text, image, video, audio, and graphic objects, and they reveal very different characteristics in hiding information inside them, different watermarking algorithms appropriate to each of them should be developed [9]. Among those media, the text documents show very peculiar properties: binary nature, block/line/word patterning, and clear separation between foreground and background areas. So algorithms specific to the text documents are required that meet those properties.

The text document watermarking will be an essential ingredient in these applications for the purpose of copyright protection.

We can classified watermarking in to two types: Visible watermarking and invisible watermarking

2-1.Visible Watermarks

A visible watermark is a visible translucent which is overlaid on the primary image. In *visible* digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. It is important to overlay the watermark in a way which makes it difficult to remove, if the goal of indicating property rights is to be achieved.

2-2.Invisible watermarks

In *invisible* digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to **detect** that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

In Our Algorithm we use invisible watermarking to save our picture that we published on web.

3- LSB Method

One of the common techniques is based on manipulating the least-signifcant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity [10].

This method is exactly what it sounds like; the least significant bits of the cover-image are altered so that they form the embedded information. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bitimage.

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 01000001
Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only half the bits in an image be changed.

Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message[10].

4. The Proposed Scheme

4-1.Background

The new proposed system adding the text watermarking in our case special name of Image (we chose the name not to exceed) ,the Images related with our college (college of medicine) that published in our website on Internet http://www.colmed-alnahrain.edu.iq so as we save our image publishing on Internet.

We use C++ language in writing the system and use Matlab software in Analysis the results.

4-2.TheProposed System Operations

The Add watermarking of new system has many operations:

1- Input the text watermarking to be hidden that can be done by open new file and entered directly.

2- Open –Image and split the body to blocks, we split the body in order to obtain small number of position to be easy in hide.

3- We convert text watermarking to ASCII code and then convert to Binary code

4- Divided the stream binary code to parts every part 24 bit represent three character of text watermarking.

5- Compare each part with pixels in block of palette

6- If find the pixel that equal the part of text watermarking , save the location of pixel else Let the pixel without change and take a new pixel and so on until we find the appropriate pixel.

7- In the case of a part of the watermarking does not match with any of the pixels of the palette in this case add 1 to the values of the bytes of the hidden watermarking and goto step5 and save the increment value in last location in array that we save in it the location of byte that equal the parts watermarking.

8- After save all locations of pixels that equivalent to parts of watermarking , we start hide the location in LSB in image start from location be the key of hiding.

9- The load image on Our web site (http://www.colmed-alnahrain.edu.iq) .

10- The new proposed system has a key which is used to extract the embedding text watermarking from image. We use a key, is number of position we began hide in.

4-3.TheAlgorithm of Proposed System

The following steps describe the algorithm:

```
Algorithm 1: hide text watermarking
Input : text , Image file
Output : Image file
```

Step1-Open Image (the bmp-file)

This step will open the bmp file and save header in a file and save the palette value of body in another file.

Step2- Split the body of the image file

This step will split the body image in equal blocks to use these blocks in hide text, we split the body in order to obtain small number of position to be easy in hide.

Step3-Convert text watermarking to ASCII code and then convert to Binary code .

```
Private Function DecToBin(ByValdIn As Double) As String
    DecToBin = ""
    While dIn>= 1
      DecToBin = IIf(dIn Mod 2 = 0, "0", "1") &DecToBin
      dIn = dIn \ 2
    Wend
  End Function
```

Step4- Divided the stream binary code to parts every part 24 bit represent three character of text watermarking, and compare with pixels in palette of image.

```
 For i= 1 to long of watermarking
    For j = 1 to 24
    Read bit from text watermarking

      S[j]=  bit from text watermarking
       Next j
Compare s[j]  with pixels in block of image

           Else
            Compare with another pixel
          End if
```

Step5- In the case of a part of the watermarking does not match with any of the pixels of the palette in this case add 1 to the values of the bytes of the hidden watermarking and go to step5 and save the increment value in last location in array that we save in it the location of byte that equal the parts watermarking

Step6- Start to hide location of pixels that equal the parts of text watermarking from the position that equal the key

Step7- Load the image in website.

Step8-End

This change is unnoticeable because the number of position is small and substitute in LSB.

5. Experimental Results

The proposed system has been built using visual C++ and can run on Pentium 3 computer and above, the setting of screen must be 800 X 600.

The results of the proposed system has been illustrated in the following

Example1:

Figure (1) Image of the garden in our college

We add text watermarking that special name (gar.jpg)

Figure (2) Image of the garden in our college after adding Watermarking

Example 2:

Figure (3) image for college carnival

We add text watermarking that special name (gar2.jpg)

Figure (4) image for college carnival after adding text watermarking

6-Experimental Results And Performance Analysis

Use PSNR Function to Test the results

Signal to Noise Ratio (PSNR) is generally used to analyze quality of image, sound and video files in dB (decibels). PSNR calculation of two images, one original and an altered image, describes how far two images are equal. Figure 5 shows the famous formula.

MSE: Mean-Square error.
x: width of image.
y: height.
x*y: number of pixels (or quantities).

This function displays the PSNR (peak signal-to-noise ratio) between two images. The answer is in decibels (dB).

PSNR is very common in image processing. A sample use is in the comparison between an original image and a coded/decoded image. Typical quoted PSNR figures are in the range +25 to +35dB.

The syntax for this file is PSNR(A,B), where A and B are MATLAB Intensity Images, with matrix-elements in the interval [0,1]

$$PSNR(dB) = 10 * \log(\frac{255^2}{MSE})$$

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{\left(\left|A_{ij} - B_{ij}\right|\right)^2}{x * y}$$

Figure5.PSNR formula.

In watermarking. We asked each one of them of she/he could tell a watermarked image if they are presented with a pair of same size images printed on a piece of paper, one watermarked and the other not. None could tell the watermarked image from the non-watermarked image.

In order to observe the image quality of watermarked image objectively, the PSNR (Peak Signal to Noise Ratio) value of the image is calculated using the equation 3 and if the PSNR value is greater than 35dB, the watermarked image is within acceptable degradation levels.

$PSNR = 10\times \lg((2n - 1)2 / MSE)$ (3)

Where n means the number of bits per sample value, the MSE represents mean square error between the host image and the watermarked image.

By using Matlab we input figure(1) and figure(2) to function PSNR the results equal 31.672 db and this value acceptable.

By using Matlab we input figure(3) and figure (4) to function PSNR the results equal 28.223 db and this value acceptable.

7. Conclusion

The proposed system proved to be a good system used to hide a text watermarking in image by divided the binary code of text watermarking to parts each parts equal to 24 bits and compare it with pixels of palette in image and save the locations of pixels equivalent in image.

- The text watermarking is short therefore easy to find is equivalent to it in pixel of Image and easy to hide it.
- The presence of key makes it difficult anyone removes watermarking.
- In the proposed system don't change anything in the pixels that hide in it but change in another pixels in which the security of system is increased,
- The proposed system proved to be easy to use and efficient in terms security and help me to save ownership of my image that published in web.
- Statistical analysis proved the admissibility of the proposed system.

6-References

[1] S. Katzenbeisser, F. A. P. Petitcolas. “Information hiding techniques for steganography and digital watermarking”, Artech House Publishers, 2000.

[2] W. Puech, J. M. Rodrigues. “A new crypto-watermarking method for medicalimages safe transfer”. In Proceedings of the 12th European Signal Processing Conference, Vienna, Austria, 2004, pp. 1481-1484.

[3] Rodríguez-ColínRaúl, Feregrino-Uribe Claudia, Trinidad-Blas Gershom de J. “Data Hiding Scheme for Medical Images” , *National Institute for Astrophysics, Optics and ElectronicsLuis Enrique Erro No. 1, Sta. Maria Tonantzintla, Puebla, Mexico C.P. 72840*

[4] D. Soumyendu,D.Subhendu,B.Bijoy, “Steganography and Steganalysis: Different Approaches” , Information Security Consultant

[5] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3, “Information and Computer Security Architecture (ICSA) Research Group” ,epartment of Computer Science
University of Pretoria, 0002, Pretoria, South Africa

[6] Moerland, T., “Steganography and Steganalysis”, *Leiden Institute of Advanced Computing Science*,www.liacs.nl/home/ tmoerl/privtech.pdf

[7] AdamMaksimuk ,”Steganography: A Tool for Evil a Tool for Good”

[8] A. Bhattacharjya and H. Ancin,"Data embedding in text fora copier system" *Proceedings of the ICIP*, Vol.2, pp.245-249, 1999.

[9] F. Hartung and M. Kutter, "Multimedia watermarkingtechniques,", *Proceedings of the IEEE*, Vol.87, No.7,pp.1079-1107, July 1999.

[10] Chi-Kwong Chan⁎, L.M. Cheng, “Hiding data in images by simple LSB substitution” , Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong KongReceived 17 May 2002; received in revised form 11 July 2003; accepted 11 August 2003

[11]MamtaJuneja, Parvinder S. Sandhu, andEktaWalia, “Application of LSB Based SteganographicTechnique for 8-bit Color Images”,, page 1,2009