A Text Watermarking Algorithm Based on LSB Method in Hiding Data

Assistant Lecture - Orooba Ismail Ibrahim
Al-Nahrain University\ College of Medicine
M.Sc. in Computer Science- Data security

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.

Add text watermark and image watermark to your photos or animated image, protect your copyright avoid unauthorized use.

In this paper was presented a watermarking scheme that hides watermarking in method, not affect the image quality.

In this work was used Small text as a watermark to embed in images is published on the website to maintain ownership of the owner website.

In this work was used LSB method in hiding operation by special techniques depend on hide the location of character but not character itself ,after finding what equivalent to its value in the a palette image and hide the position of palette equivalent value of the site

After hiding watermarking, published the image in website .

By using this Algorithm , images are published on the Internet while retaining ownership of the images , and knowledge of the images reproduced without the owner's knowledge.

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

المستخلص

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 يتم تقديم نظام علامة مائية يخفي العلامة المائية بطريقة لاتؤثر على جودة الصورة.
في هذا العمل تم استخدام نص صغير كعلامة مائية يخفى في الصورة المنشورة في الموقع الالكتروني للحفاظ على ملكية الصور الخاصة بموقع مالك الصورة .
في هذا العمل ، تم استخدام طريقة البتات الاقل اهمية لكن بطريقة جديدة تعتمد على اخفاء مواقع الحرف وليس الحرف نفسه بعد ايجاد ما يكافيء قيمته في البلت للصورة واخفاء موقع قيمة البلت المكافيء.
بعد اخفاء العلامة المائية في الصورة يتم نشر الصورة في الموقع .
باستخدام هذه الخوارزمية يتم نشر الصور على الانترنيت مع الاحتفاظ بملكيتها ، ومعرفة الصور التي تم استنساخها دون معرفة مالك الصورة .

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 [2].

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 the watermarking indirectly in image by hide the position of pixel in palette that their value equal to Asscii value of character in watermarking.

2. Watermarking

Steganography and watermarking are main parts of the fast developing area of **information hiding** [4].

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 [5].

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 [2]. 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.

Watermarking could be in classified 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 is also possible to use hidden embedded information as a means of covert communication between individuals.

The proposed Algorithm an invisible watermarking were used to save the picture that were 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 [6].

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.

A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable. Other variations on this technique include ensuring that statistical

changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. Changes in these pixels are then avoided because slight changes would cause noticeable variations in the area.

While LSB insertion is easy to implement, it is also easily attacked. Slight modifications in the color palette and simple image manipulations will destroy the entire hidden message [6].

4. The Proposed Scheme

The new proposed system adding the text watermarking in our case special name of image (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 in our case an 8-bit image and since 8-bit image and 8-bit values can only have a maximum of 256 colors [7].

5- The Proposed Scheme Operation

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- Find the position where to hide the bytes of the text in the blocks of image and store the block numbers and the number of position in file to be use later.
4- Substitute the character in the position get from the search program, in fact the substitution it merely locate the position that hide in it.
5- Hide position will hide the block numbers where the character was hidden.
6- Combine the blocks into a one file and then combine the header and the body file into a file to perform the Image (bmp file).
7- The load image on Our web site (http://www.colmed-alnahrain.edu.iq)

The new proposed system has a key which is used to extract the

embedding text watermarking from image. We use a key, as number's position we began hide in.

5.1- The Algorithm of the Proposed System

The following steps describe the algorithm:

Algorithm 1: Split the Image

Input : Image

Output : Array of binary code

Open Image (the bmp-file) Operation.

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

2- Split the body of the image file operation (each part 300X 300).

This operation will split the body image in equal blocks (300 x 300) to use these blocks in hide text, we split the body in order to obtain small number of position to be easy in hide.

3- save the value of pixel palette in array

4-End

algorithm 2: find the position

Input : Array of binary code of image , Ascii code for text watermarking

Output : positions of pixel that equal to Asccii code of text image

---

1- Find the position operation this operation is done by read a block from block image file

2- Test if block is suitable to hide a byte from text file or not. The testing is done by compare the value of the palette with ASCII value of character.

3- If value of the palette equal with ASCII value of Character, this mean we find the position that we hide the character and save the block number and position in a file.

4- End

Algorithm 3: Substation

Input : Array of binary code of image , Ascii code for text watermarking

Output : positions of pixel that equal to Ascii code of text image

Substitute the character operation this operation is done by read character from text file and locate the position where to hide the character in the block.

1- Replace the character in specific position and hide the position of the replaced character in the first row and last row of the block.
2- This change is unnoticeable because the number of position is small and substitute in LSB.
3- End

6- Extracting The text Watermarking

Extracting the text is done by using the key stored into first block position that contains the Key.

Later get the row position from the first row and convert the binary value to a decimal value and in the same way we position by applying the following equation

Pos =(r+1) * 20- (20-c)Get the character value from the specific position.

6.1- The Algorithms of Extracting

The following steps describe the algorithm:

Algorthim 1: Image

Input : Image

Output : Array of binary code

1- Open the bmp file by reading the header and getting the body of the file
2- Split the file into blocks (300 x 300).
3- by using the key get the first block that contains the first byte of the text.
- For I= 1 to the length of the message do
- Find the position of the embedded character from the first and the last row of the block.

Get the row position from the first row.

Convert the binary value to a decimal value.

Get the column position from the last row

Convert the binary value to a decimal value, get the position by applying the following equation:

Pos =(r+1) * 20- (20-c)

Get the character value from specific position.

- From the current block find the position of the next block.

The number of the block is hidden in the first row and the second half of the last row.

- The end

7. 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 with special name (garden1)

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

Example 2:

Figure (3) image for college carnival

We add text watermarking with special name (Student Safa)

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

8-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]

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

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

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 28.722 db and this value acceptable.

By using Matlab we input figure(3) and figure (4) to function PSNR the results equal 30.323 db and this value acceptable

9. Conclusion

The proposed system proved to be a good system used to hide a text watermarking in image by compare value of palette with ASCII of character and if equal we hide position in another Place.

- 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, in case the third person explore anything in picture he explore

- The proposed system proved to be easy to use and efficient in terms security and help to save ownership of an image that published in web.

10-References

[1] S. Katzenbeisser, F. A. P. Petitcolas. "Information hiding techniques for steganography and digital watermarking", Artech House Publishers, pp,220, December ,2000.

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

[3] 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.

[4] 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*

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

[6] D. Soumyendu, D.Subhendu,B.Bijoy, "Steganography and Steganalysis: Different Approaches" , Information Security Consultant

[7] 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.

[8] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3, "Information and Computer Security Architecture (ICSA) Research Group" ,department of Computer Science
University of Pretoria, 2000, Pretoria, South Africa

[9]Mamta Juneja, Parvinder S. Sandhu, and EktaWalia, "Application of LSB Based SteganographicTechnique for 8-bit Color Images",, page 1,2009

[10] AdamMaksimuk ,"Steganography: A Tool for Evil a Tool for Good"

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