# New Data Hiding Methods for Copyright Protection, Annotation, and Authentication of BMP Archive Images in Digital Libraries and Museums

Chih-Yang Yin, Da-Chun Wu and Wen-Hsiang Tsai

ᵾDepartment of Computer and Information Science
National Chiao Tung University
Hsinchu, Taiwan 300

Department of Computer and Communication Engineering
Ming Chuan University
Taipei, Taiwan 111

## Abstract

Data hiding techniques for copyright protection, annotation, and authentication of BMP archive images in digital libraries and museums are proposed. After artworks preserved in libraries and museums are digitized, the copyright of them need be protected. A method for embedding watermark signals within BMP images is proposed to prove its copyright owner. To embed annotation data within BMP images for easy association of image annotations, a novel method for embedding boundary line signals, which can be used for localizing starting points of annotations within stego-images, is also proposed. Finally, a method for embedding anti-cropping fragile signals within BMP images for image authentication to verify image integrity and fidelity is proposed. Good experimental results prove the feasibility of the proposed methods.

Keywords: stego-image; fragile watermarking; image authentication; annotation hiding; Digital watermarking

## 1. Introduction

Data hiding is a technique developed for embedding imperceptibly secret information behind certain data. In this study, we study embedding secret data behind images. The secret information may be texts, images, videos, or any other type of data. The image used to hide the secret is called a *cove image* and the resulting image is called the *stego-image*. Because the embedded information is certain secret data, the quality of the stego-image is the most important requirement; it is desired that no obvious visual artifacts will be observed in the stego-image. In this study, it is aimed to develop effective data hiding methods for applications in digital libraries and museums, including copyright protection, annotation, and authentication of archive images in the BMP form.

### 1.1 Survey of Data Hiding Methods

Many different methods have been proposed data hiding in images during the last few years and most of them can be seen as substitution systems. Such methods try to substitute redundant parts of images with the secret information. The least-significant bit (LSB) method [1] proposed by Adelson in 1990 embedded secret data by replacing the least-significant bits of image pixels. Since

only minor modifications are made in the embedding process, the sender assumes that a passive attacker will not notice the change. Liaw and Chen [2] proposed an approach which is based on gray value replacement. Each pixel in a secret image is embedded in a cover image by replacing a pixel in the cover image with a similar pixel value. The LSB method is easy and fast to implement and a surprising amount of information can be hidden with little perceptible distortion to the image. But the LSB method is rather brittle and vulnerable to corruption due to small changes to the image.

Recently, the development of new robust watermarking techniques led to advances in the construction of robust and secure image data hiding systems. Chen, Chang, and Hwang [3] proposed a virtual image cryptosystem for encrypting an image into another based on a vector quantization technique. Wu and Tsai [4] proposed an image data hiding method based on image differencing. A difference value is calculated from every non-overlapping pixel pair of the cover image. All possible difference values are quantized into a number of ranges. The selection of the range intervals is based on the characteristic of human vision's sensitivity to gray value variations from smoothness to contractiveness. The difference value is then replaced by a new value to embed the value of a sub-stream of the secret message. This method provides an easy way to produce a more imperceptive result than those yielded by LSB methods. Chang and Tsai [5] proposed an image data hiding method based on the wavelet transform. The secret message is embedded within the cover image by replacing the middle and high frequency wavelet coefficients. In the method proposed by Yen and Tsai [6], both the cover image and the secret image are transformed into the frequency domain, and a DCT coefficient replacement method is then utilized to accomplish the hiding process.

### 1.2 Techniques for Image Watermarking

Many techniques about embedding robust watermarks in images for copyright protection have been proposed in recent years. A watermark could be a serial number, a copyright logo, a random signal, or any image-adaptive value created by the watermarking procedure. Image watermarking techniques proposed so far can be categorized into two main types: the spatial-domain watermark and the frequency-domain watermark.

The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudorandom noise pattern to the luminance values of its pixels. Many methods are based on this principle [7, 8]. The patchwork method [9] changes the gray values of pixels by adding a value to the gray values of one set of pixels while subtracting the same value from another set. The image watermark may be embedded in the frequency domain, too. In the method proposed by Koch and Zhao [10], a random sequence pulse position codes are used to embed the watermark. Chang and Tsai [5] embedded a watermark logo in the wavelet domain by changing the relationship of low

frequency coefficients. A DCT-based method for embedding the watermark signal in the DCT coefficients was proposed by Hsu and Wu [11]. In the method proposed by Barni, Bartolini, Cappellini, and Piva [12], and Cox, Kilian, Leighton, and Shamoon [13], secure spread spectrum methods were applied in the watermarking procedure. Methods that embed the watermark in the frequency domain tend to be more complicated than methods used in the spatial domain, but they are more robust.

Some robust watermarking techniques exploit the characteristics of the human perceptive capability to guarantee that the modification made to the given image is imperceptible. Wu and Tsai [14] proposed a method to embed watermark logos based on a human visual model. The given image is first partitioned into subimages. The watermark information is embedded by properly adjusting the gray values of the pixels in the central region of each subimage so that the mean gray value of them is equal to some chosen extreme values.

### 1.3 Techniques for Image Authentication

In the recent years, proposed systems that are used for verifying the authenticity of a digital image may be categorized, according to the nature of the employed approaches, into two types, the signature system [15] and the fragile watermark system. In a signature system, a digest of the data to be authenticated is obtained by the use of cryptographic hash functions. The recipient verifies the signature by examining the digest of the data and using a verification algorithm to determine if the data is authentic. A disadvantage of the signature system is that the additional signature must be stored and transmitted separately from the protected image. A fragile watermark system, on the contrary, embeds the authentication information inside the image and provides the ability to localize the altered areas within the image. Fragile watermark systems can be classified into two types, spatial-domain fragile watermarking system or transformed-domain watermarking one.

The method proposed by Walton [16] embeds a watermark in the least-significant bit plane for perceptual transparency. Another method proposed by van Schyndel [17] used check-sums information as the watermark message which is also embedded into the LSB plane. Wong [18] partitioned images into blocks and used the LSB plane of each block for embedding watermark information. The information is generated by a cryptographic hash function which uses the pixel values of all pixels in a block and the dimension information of the image as the parameters. Wu and Tsai [19] proposed a method for embedding perception-based fragile watermarks. A human visual model is employed to guarantee that modifications in images are imperceptible. And the watermark value is embedded in the image by replacing the gray value of the central pixel of every 3×3 image block.

About the methods that embed fragile watermarks in the transformed domain, Fridrich [20] divided an image into 64×64 blocks, and inserted a watermark value into each block by modifying the middle third of

the DCT coefficients of each block. Wu and Liu [21] described a technique based on a modified JPEG encoder. The watermark is inserted by changing the quantized DCT coefficients before entropy coding. One wavelet-based technique based on Harr wavelets was proposed Kundur and Hanzinzkos [22], which was shown to be tolerant with high quality JPEG compression. A wavelet decomposition of an image contains both frequency and spatial information about the image, and hence watermarks embedded in the wavelet domain have the advantage of being easy to locate and being effective for use to characterize illicit tampering.

### 1.4 Brief Description of Proposed Approach

After artworks preserved in libraries or museums are digitized as images, protection of their copyright and the annotation data associated with them becomes important. In this study, new techniques for this purpose are proposed. An archive image is defined in this study as a digital image that is primarily used for preservation in the libraries or museum database and for reproduction of reference and thumbnail images in applications of digital libraries or museums. The digitized works should be archived in a digital file format that stores the image in full colors, high quality, and without any loss or distortion. Because archive images are assumed not to be exposed on the Internet environment, the file size of an archive image is not an important consideration. Under these considerations, the BMP (Bitmap) image format hence becomes a good choice for the archive image, as is adopted in this study.

In the applications of digital libraries and museums, almost every digitized image has some related annotation, which includes descriptions or documents about the art. Embedding the annotation inside the image will greatly reduce the work about matching the image with its descriptions, especially when images become plenty. Delivery of the image will also be more convenient because the image and its annotation are combined together and can be transmitted simultaneously. In Section 2, an annotation-hiding scheme for archive images is proposed.

Digital watermarking is a technique for protecting the copyright of image owners. It embeds a signal (called a watermark) into a cover image in a way that yields imperceptible results under normal observation. In Section 3, a scheme for embedding a museum logo, as the watermark, is proposed.

A fragile watermarking method is proposed in this study. Fragile watermarking is one of the techniques developed for image authentication, which aims to verify the integrity and fidelity of an image. A fragile watermark is a kind of watermark that is designed to be easily destroyed when the watermarked image is manipulated. Image authentication can be achieved by inspecting whether the embedded signal is destroyed. In this study, a human visual model is utilized to ensure perceptual invisibility of the embedded mark. And a new method is also

proposed to embed boundary line signals within an image to assist locating the starting point of annotation data in the authentication process. The details will be described in Section 4.

## 2. Proposed Annotation Hiding Scheme by Replacement of LSB Bits

In this section, the proposed scheme of annotation data hiding is described, including the process of embedding annotation data into a BMP image and the reverse process of extracting them. The LSB method is adopted here for the data embedding purpose in consideration of its simplicity, capacity, and embedding speed. Some experimental results will also be shown.

### 2.1 Proposed Annotation Data Embedding Process

The annotation data associated with a given cover image are embedded within the blue channels of the image in the proposed method. Two LSB's of each pixel in the cover image are utilized to carry the annotation data bits. More specifically, in the proposed data embedding process, the input cover image is first divided into non-overlapping 3×3 image blocks. Every two bits $B_1$ and $B_2$ of the annotation data are then embedded into a cover image pixel $P$ by replacing the values of the two LSB's of each of the eight surrounding pixels of $P$ with $B_1$ and $B_2$, as illustrated by Fig. 1. The values of the central pixels of the image blocks are left unchanged to embed signals of the fragile watermark and boundary lines, as described in Section 4.

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | | 5 |
| 6 | 7 | 8 |

Figure 1. An example of 3×3 image block with eight surrounding pixels for annotation data embedding by LSB replacement.

Furthermore, the proposed method in this paper is able to embed as many copies of the annotation data as possible in the cover image for best space utilization and retrieval reliability. For this, each copy of the annotation data is embedded within a square area composed of 3×3 image blocks. In corporate with the boundary lines that are embedded along with the fragile watermarks, which will be described in Section 4, the annotation data can be extracted with high probability even when the stego-image is cropped. Fig. 2 shows a diagram that illustrates the hiding position of the annotation data and the boundary lines within a cover image. In the diagram, every cell represents a 3×3 block of the cover image. The gray blocks are the boundary lines that will be used for locating the start position of the embedded annotation. The white blocks are used for embedding the annotation data. In this study, every 3×3 block will be used for embedding two bytes of annotation data, if the annotation data has $L$ characters in length, $\left\lceil \frac{L}{2} \right\rceil$ 3×3 blocks are needed to embed a copy of annotation. So,

the border width $B$ of the square area used for embedding a full copy of annotation data can be computed as follows:

$$B = \left\lceil \sqrt{\left\lceil \frac{L}{2} \right\rceil} \right\rceil. \quad (1)$$

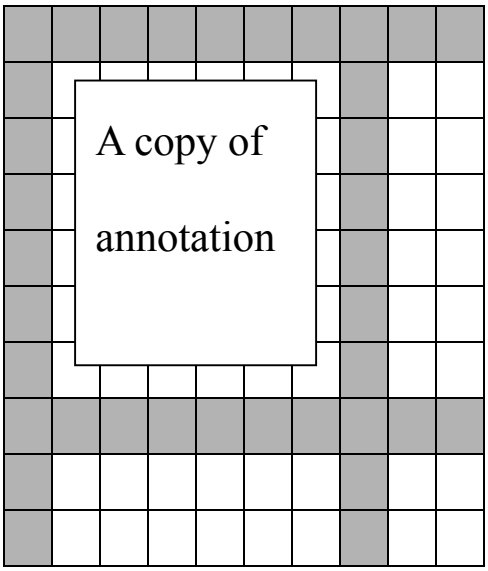



Figure 2. The diagram of annotation hiding position

Therefore, $B^2$ blocks that comprise a square area will be used to embed a copy of annotation data. So, $\alpha$ copies of annotation data that can be embedded within a cover image can be calculated as follows:

$$\alpha = \left\lfloor \frac{M}{B+1} \right\rfloor \times \left\lfloor \frac{N}{B+1} \right\rfloor, \quad (2)$$

where $M$ and $N$ are the width and the height of the cover image, respectively.

Let $C$ be the cover image of size $M \times N$. Let $S$ be the annotation with $L$ characters in length that we want to embed into $C$. The entire embedding algorithm can be briefly expressed as follows.

Step 1: Divide the cover image $C$ into non-overlapping 3×3 blocks. The annotation data will be embedded in the eight surrounding pixels of every 3×3 block by replacing two LSB's of the pixels.

Step 2: Compute the border width $B$ of the square area that will be used to really embed the annotation data as follows:

$$B = \left\lceil \sqrt{\left\lceil \frac{L}{2} \right\rceil} \right\rceil.$$

Step 3: Compute the total number of annotation copies $\alpha$ that can be embedded within the cover image $C$ by

$$\alpha = \left\lfloor \frac{M}{B+1} \right\rfloor \times \left\lfloor \frac{N}{B+1} \right\rfloor.$$

Step 4: Convert the annotation data S into binary form $S = (s_1 s_2 \mathrm{K}\ s_7 s_8 \mathrm{K}\ s_{(8\times L)})_2$

Step 5: Replace two LSB's of the pixels, which are within the square area, by two bits of the annotation data $S$ repeatedly, until all of the binary data in $S$ are embedded.

Step 6: Repeat Step 5 for $\alpha$ times to embed the annotation data S within the pixels of different square areas.

The boundary lines which separate the square areas are embedded later within the cover image $C$ together with the fragile watermark, which will be described in Section 4.

## 2.2 Proposed Annotation Data Extraction Process

In the annotation extraction process, no other information but the embedded image is needed. Because many copies of annotations are embedded within a stego-image and they are separated by the boundary line signals. The first step in the extraction process is to find out the signals. The process of searching the boundary lines within the stego-image will be described in Section 4. Two consecutive horizontal and vertical boundary lines must be found to decide the border length of a square area, where the annotation data is embedded. Fig. 3 shows that a square area that can be located when two consecutive horizontal and vertical lines are found.

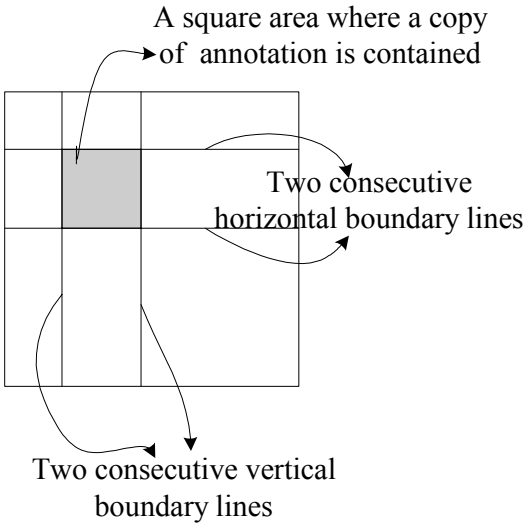



Figure 3. A diagram that illustrates the searching process of a square area.

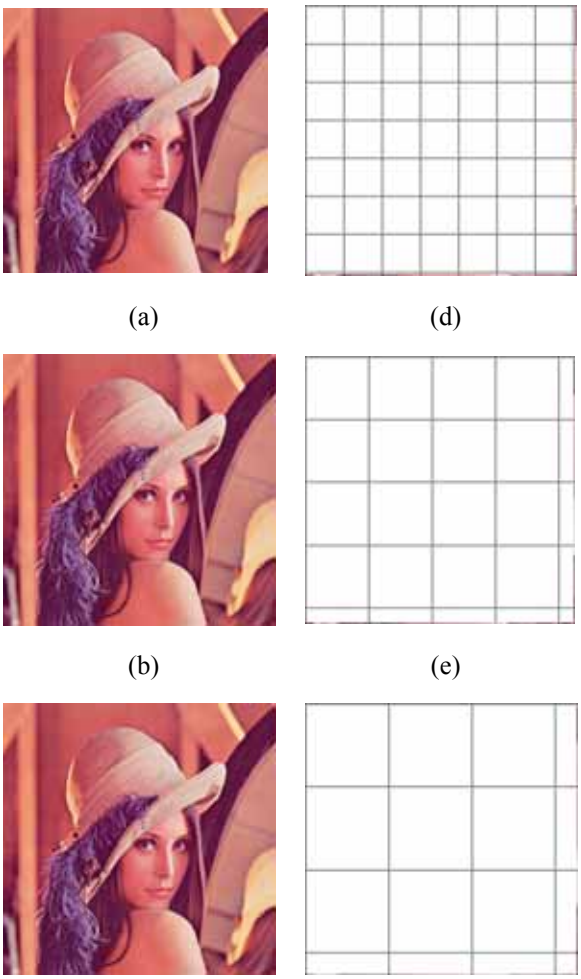
If the location of a square area can be determined, the annotation embedded within the square area then can be easily extracted. The square area is first divided into non-overlapping 3×3 blocks. The annotation data are extracted block by block. For every 3×3 block, the annotation can be extracted from two LSB's of the surrounding eight pixels in the order shown in Fig. 1. For every 3×3 block, two bytes of data can be extracted. After all of the blocks are exhausted, convert the extracted binary-form annotation data into characters. So, the embedded annotation data are obtained.

## 2.3 Experimental Results

In our experiments, the image "Lena" as shown in Fig. 4 with size 512x512 is used as a cover image. The images that resulted from embedding 1000, 3000, and 5000 characters are shown in Figs. 5 (a), (b), and (c), respectively. The PSNR values of the stego-images are shown in Table 1. Figs. 5 (d), (e), and (f) show the boundary lines that are embedded within the stego-images. The lines with gray color in the figures are the boundary line information which are used for separating each copy of the embedded annotation and the white block are the square areas where the annotation data are embedded. The shorter the annotation is, the more copies of them can be embedded. 49 copies of annotation can be embedded within the cover image when the data are 1000 characters in length. 9 copies can be embedded when the data are 5000 characters in length.

Fig. 6 shows a cropped version of Fig. 4. Even the stego-image is cropped, the start position of a square area still can be found, so the annotation can be extracted correctly with the help of the boundary lines.

Figure 4. The cover image “Lena”.



(a) (d)

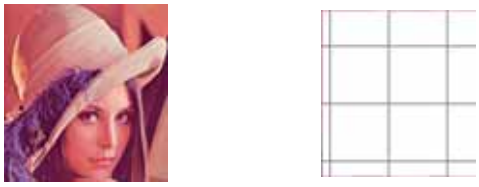
(b) (e)

(c) (f)

Figure 5. The stego-images after embedding different copies of annotation with different lengths and the boundary line information that is used to separate the square areas. (a) 49 copies of 1000 characters embedded. (b) 16 copies of 3000 characters embedded. (c) 9 copies of 5000 characters embedded. (d) - (f) Boundary lines that separate the square areas.

Table 1. The PSNR values of the stego-images with different annotation lengths and numbers of copies.

| | 1000 characters 49 copies | 3000 characters 16 copies | 5000 characters 9 copies |
|---|---|---|---|
| PSNR | 43.0 | 42.9 | 43.1 |



(a) (b)

Figure 6. The cropped stego-image and its corresponding boundary line information. (a) A cropped version of Figure 4. (b) Boundary lines and square areas.

## 3. Proposed Watermarking Scheme by Replacement of LSB Bits

In this section, the process of embedding a binary logo image within an archive image will be described. A logo image (for example, a museum logo) here is treated as a watermark to prove the ownership of the watermarked image. In the applications of digital museums, the archive images are not exposed in the Internet environment, it is presumably impossible for an archived image to be stolen. The robustness of the watermark hence is not a major consideration. The quality of the watermarked image, on the contrary, is a more important issue. The insertion of the watermark should not cause much distortion to the archive image since it will be used for preservation.

### 3.1 Proposed Watermark Embedding Method

Let $C$ be a cover image of size $M \times N$, and $L$ be a binary logo image of size $I \times J$ that will be embedded within $C$. Since $L$ is a binary image, $L$ can be transformed into binary form $L = (l_1\, l_2\, l_3 \ldots l_{I\times J})_2$ before embedding. In the proposed embedding process, the logo image $L$ will be embedded by replacing one LSB of the pixel in the cover image. The information about width and height ($I$ and $J$) of the logo image will be first converted into a binary stream and embedded within the cover image firstly. After $I$ and $J$ are embedded, we then start to embed $L$ by replacing one LSB of each pixel in the cover image, one pixel a time and sequentially, until all bits in the logo image $L$ are exhausted.

### 3.2 Proposed Watermark Extraction Process

No other information but the stego-image is needed in the watermark extraction process. Before extracting the logo image data, the width and height information of the logo must first extracted from the stego-image so that we can know how many pixels should be extracted before starting the extraction process. The width and height information is extracted from one LSB's of each of the pixels in the left-up corner of the stego-image. Let $I$ and $J$ be the extracted width and height of the logo image, respectively. Then the logo binary data can then be extracted from the LSB's of the $I \times J$ pixels in the stego-image sequentially. Let $L = (l_1\, l_2\, l_3 \ldots l_{I\times J})_2$ be the extracted logo binary data. In cooperate with the width and height information $I$ and $J$, the embedded binary logo can be then reconstructed.

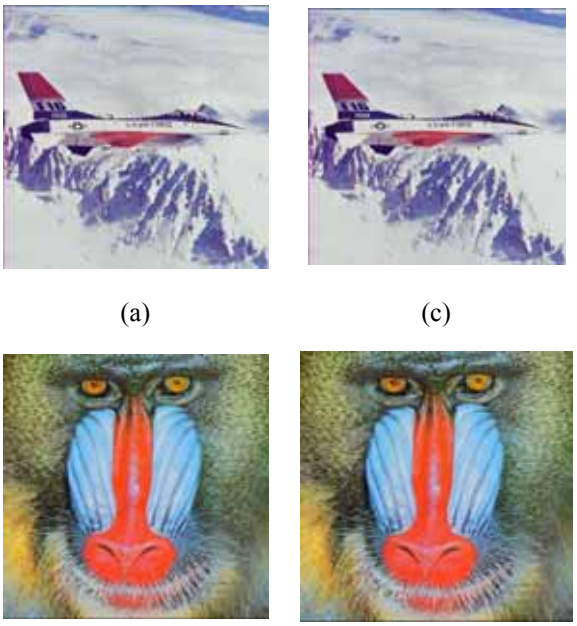
### 3.3 Experimental Results

In our experiments, the copyright logo of a digital museum of size 256 × 256, which is shown in Fig. 7, is embedded into the images as shown in Figs. 8 (a), and (b) with size 512 × 512. Figs. 8 (c) and (d) are the stego-results. The PSNR values of the stego-images are shown in Table 2. No difference can be found visually between the cover and corresponding stego- images and the PSNR values are high.

Figure 7. The copyright logo of a digital museum.

Table 2. The PSNR values of the images after embedding the copyright logo of the digital museum.

| | Jet | Baboon |
|---|---|---|
| PSNR | 45.4 | 43.0 |



(a) (c)

(b) (d)

Figure 8. The cover images and the stego-images after embedding the logo image of Fig.7. (a) Cover image "Jet". (b) Cover image "Baboon". (c) - (d) Images after embedding Fig. 7.

## 4. Proposed Authentication Scheme by A Human Visual Model

In this section, a method for embedding fragile watermarks in archive images based on a human visual model, which is proposed in [19] will be described. The human visual model is employed to guarantee that the modification of images in the fragile watermark embedding process is imperceptible. And another signal, called "the boundary line" proposed in this study, will also be embedded together with the fragile watermark. With the help of the boundary lines, every copy of the embedded annotation inside a square area, which was described in Section 2, can be separated. Any alteration of the watermarked image can be verified and localized by examining the fragile watermark and the authentication can be accomplished without referencing the original image. In Section 4.1, the human visual model adopted in the watermark embedding process will be first introduced. And the watermark embedding process will be described. In Section 4.2, the process for searching the boundary lines will be described. In Section 4.3, the process of authenticating a suspicious image will be described. Finally, some experiments will be shown in Section 4.4.

### 4.1 Fragile Watermarking and Boundary Line Embedding Process

The human visual system has been studied for years in the field of image coding and compression. Some of the proposed human visual systems have the ability to calculate some thresholds called JND (Just-noticeable distortion) or TEL (tolerable-error level) by the gray value of a pixel and its background intensity. Any change to the gray value between the threshold ranges is considered to be imperceptible. In this section, a human visual model proposed in [19] is utilized to embed the fragile watermark and the boundary line information.

Before the embedding process starts, the original image is first divided into non-overlapping 3×3 image blocks. The eight surrounding pixels of a 3×3 image block are considered as the background of the central pixel. In the embedding process, the standard deviation $\sigma$ of the eight surrounding pixels is first calculated. The

human visual model takes σ as a parameter and classified the 3×3 blocks into four classes, from smooth areas to edged areas. The contrast function of the central pixel is then decided by equally quantizing the gray values into *n* levels according to which class it is assigned to. The criteria used to categorize the classes of the background and the quantization levels are shown in the following:

$$\text{the number of the quantization levels } n = \begin{cases} 32 & \text{when } \sigma \le 2.4; \\ 24 & \text{when } 2.4 \le \sigma \le 3.6; \\ 16 & \text{when } 3.6 \le \sigma \le 4.8; \\ 12 & \text{when } 4.8 \le \sigma. \end{cases} \quad (3)$$

Let $g$ be the gray value of the central pixel. $g$ will definitely fall within one of the quantization levels, say $L$, defined by two visual thresholds, say $g_{\min}$ and $g_{\max}$. From the viewpoint of the adopted human visual model, this means that any gray value in the range $L$ will have the same sensitivity under the same background with standard deviation σ. That is, if we replace $g$ with a gray value in range $L$, the modification will be imperceptible.

| | | |
|---|---|---|
| 136 | 138 | 129 |
| 136 | 138 | 129 |
| 136 | 138 | 129 |

Figure 9. A 3×3 block and its gray values.

Take Fig. 9 as an example. The standard deviation of the eight surrounding pixels is about equal to 3.95. According to the classification criteria, the contrast function values of the central pixel will be equally quantized into 16 quantization levels. And the gray value 138 of the central pixel falls within the quantization level range from 128 to 143. This means that if we replace the gray value of the central pixel with any value from 128 to 143, the modification is imperceptible.

With the help of the human visual model, the fragile watermark and the boundary line information can be embedded in the central pixel of every 3×3 image block. The detail is described as follows.

Step 1: Let $C$ be the original image with size $M \times N$. Divide $C$ into non-overlapping 3×3 blocks, and label coordinates $(X, Y)$ to every block according to its position within $C$, where $0 \le X \le \left\lfloor \frac{M}{3} \right\rfloor - 1$ and $0 \le Y \le \left\lfloor \frac{N}{3} \right\rfloor - 1$. Fig. 10 shows the 3×3 blocks with allocated coordinate $(X, Y)$.

| | | | | |
|---|---|---|---|---|
| (0,0) | (1,0) | (2,0) | (3,0) | |
| (0,1) | (1,1) | (2,1) | (3,1) | |
| (0,2) | (1,2) | (2,2) | (3,2) | |
| (0,3) | (1,3) | (2,3) | (3,3) | |
| | | | | |

Figure 10. 3x3 blocks with allocated coordinates (X,Y).

Step 2: For every 3×3 block, calculate the standard deviation $\sigma_{(X,Y)}$ of the

background to determine which class the block belongs to. And the range $L = \{g_{\min(X,Y)}, g_{\max(X,Y)}\}$ of the quantization level can be obtained according to the gray value $g_{(X,Y)}$ of the central pixel.

Step 3: The border length $B$ of the square area, which is described in Section 2, is important information in this step to determine whether the fragile watermark or the boundary line signal should be embedded in the central pixel of 3×3 block. For every 3×3 block, modify the gray value of the central pixel by the following conditions:

$$g'_{(X,Y)} = \begin{cases} g_{\min(X,Y)} + \alpha, & \text{if } X \bmod (\mathrm{B}+1) = 0 \\ & \text{or if } Y \bmod (\mathrm{B}+1) = 0; \\ g_{\min(X,Y)} + \beta, & \text{otherwise;} \end{cases} \quad (4)$$

where $g_{\min(X,Y)} + \alpha < g_{\max(X,Y)}$ ,

$g_{\min(X,Y)} + \beta < g_{\max(X,Y)}$ , $\alpha \neq \beta$ ,

and $\alpha$ and $\beta$ are constants that indicate whether the boundary line signal or the fragile watermark are embedded. That is, the central pixel of a 3×3 block is replaced by $g_{\min(X,Y)} + \alpha$ to indicate that the boundary line signal is embedded. Otherwise, we replace the gray value of the central pixel by $g_{\min(X,Y)} + \beta$ to indicate that the fragile watermark signal is embedded. The selection of the values of $\alpha$ and $\beta$ should ensure that the embedding result will not make any visible distortion to the watermarked image.

### 4.2 Boundary Line Searching Process

In the process of searching a vertical (or horizontal) boundary line, the adopted human visual model is utilized to examine whether the boundary line signal is present in the 3×3 image block. A 3×3 block mask is used to determine whether a boundary line signal exists. The algorithm can be briefly expressed as follows.

Step 1: For every masked 3×3 image block, compute the standard deviation $\sigma$ of the background. The quantization level range $L = \{g_{\min}, g_{\max}\}$ of the central pixel g can also be obtained from the human visual model. The boundary line signal is decided to be present if the following condition holds:

$$g = g_{\min} + \alpha \quad (5)$$

where $\alpha$ is a constant and $g_{\min} + \alpha < g_{\max}$. That is, if the gray value of $g$ satisfies the constraint defined in Eq. (5), then we judge that the boundary line signal is contained in that block. We start the searching process from the left-top 3×3 block of the image. If the boundary line signal does not exist,

we move the mask one pixel to right (or down) in an overlapping manner until the first block that contains the boundary line is found.

Step 2: To ensure that the boundary line does really exist, we must examine some more 3×3 blocks to make sure of it. We examine γ 3×3 blocks under (or to the right of) the block we found in Step 1 to observe if the boundary line signal exists. If the boundary line signal does exist in all of the γ blocks, the position of the boundary line can then be determined. Otherwise, repeat Step 1 to find another block that contains the boundary line signal.

### 4.3 Image Authentication Process

In the image authentication process, no other information but the suspicious image is needed for verifying the integrity and fidelity of the image. With the help of the boundary line signal, the proposed fragile watermark has the ability to authenticate the image even when it is cropped. Since the left-top pixel (with coordinates (0,0)) of the suspicious image may not be a starting point of the 3×3 block if it has been cropped, there will be a false authentication if we cannot decide the starting point before proceeding the authentication process. To determine the starting point for authentication, a vertical boundary line and a horizontal one must be found first by the method described in Section 4.2. Let $i_v$ be the x-coordinate of the vertical line, and $j_h$ be the y-coordinate of the horizontal line. The starting point $O$ can be then determined by

$$O = (i_v \bmod 3,\ j_h \bmod 3). \quad (6)$$

From the starting point $O$, the suspicious image is divided into non-overlapping 3×3 blocks. For every 3×3 block, the standard deviation $\sigma$ of the background is calculated and the quantization level range $L = \{g_{\min},\ g_{\max}\}$ of the central pixel $g$ is also obtained from the human visual model. The block is determined not being tampered with if $g = g_{\min} + \alpha$ or $g = g_{\min} + \beta$. That is, if the gray value of the central pixel is equal to $g_{\min} + \alpha$ or $g_{\min} + \beta$, it means that the boundary line signal or the fragile watermark is found to be present and the block is thus judged as not being tampered with.

In our experiments, a visual inspection tool for localizing any alteration in the watermarked image is provided. The blocks marked with black color are the blocks judged as being tampered with. The white and gray blocks are the blocks judged as not being tampered and as containing a boundary line, respectively.

### 4.4 Experimental Results

The images shown in Figs. 11 (a) and (b) of size 512×512 are used in our experiments. Also, the images with embedded fragile watermarks and boundary lines are shown in Figs. 11 (c) and (d). The results show that fragile watermarks can be embedded through the proposed method without noticeable changes. The PSNR values are shown in Table 3.




(a) (c)

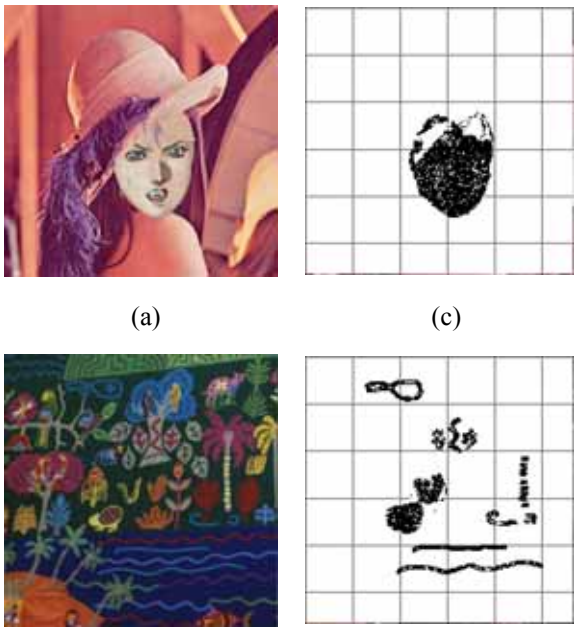
(b) (d)

Figure 11. The cover images and the watermarked images. (a) Cover image ”Lena”. (b) Cover image “Baboon”. (c) Cover image “Painting”. (d) Watermarked image “Lena”. (e) Watermarked image “Baboon”. (f) Watermarked image “Painting”.

Table 3. The PSNR values of the images after embedding the fragile watermark and boundary line information.

| | Lena | Painting |
|---|---|---|
| PSNR | 44.0 | 46.0 |

Figs. 12 (a) and (b) show some tampered images of Figs. 11 (a) and (b), respectively. Fig. 12 (a) is tampered with by replacing the face of “Lena” with another one. Fig. 12 (b) is altered by drawing some extra lines and exchanging the places of the snake and the mouse in the image. The results of authentication are shown in Figs. 12 (c), and (d), respectively. The alterations are detected with high probability and locate precisely, as shown.



(a) (c)

(b) (d)

Figure 12. Tampered images and its authentication results. (a) Tampered image “Lena”. (b) Tampered image “Painting”. (c) - (d) The results of authentication.

Fig. 13 (a) shows a tampered and cropped image. With the help of the boundary line signal, the starting point still can be found and then the image can be authenticated. Fig. 13 (b) shows the result of authentication.

(a) (b)

Figure 13. A cropped and tampered image and its authentication results. (a) Cropped and tampered image. (b) Result of authentication.

## 5. Conclusions

In this paper, a system is proposed which embeds annotation data, museum copyright logos, and fragile watermarks simultaneously within an archive image. Annotation data are embedded within eight surrounding pixels of each 3×3 image block by using the LSB replacement method. Multiple copies of annotation can be embedded. Each copy of annotation is separated by boundary line signals, which are embedded together with the fragile watermark. The annotation data within cropped images may still be extracted if any two consecutive vertical and horizontal boundary lines, which embrace a square area, can be found. A museum copyright logo can also be embedded to prove the ownership of the archive image. Finally, a fragile watermark based on a human visual model can be embedded in central pixels of 3×3 blocks imperceptibly. Any alteration to the watermarked image can be detected and located with high probability. A visual inspection tool is also provided if an image has been tampered.

## References


[1] E. H. Adelson, “Digital signal encoding and decoding apparatus,” U.S. Patent 4939515, 1990.

[2] M. S. Liaw and L. H. Chen, "An effective data hiding method," in *Proc. IPPR Conf. on Computer Vision, Graphics, and Image Processing*, Taiwan, R.O.C., 1997, pp.146-153.

[3] T. S. Chen, C. C. Chang, and M. S. Hwang, “A virtual image cryptosystem based upon vector quantization,” *IEEE Transactions on Image Processing*, vol. 7, no. 10, pp. 1485-1488, 1998.

[4] Da-Chun Wu and Wen-Hsiang Tsai, “Embedding of Any Type of Data in Images Based on A Human Visual Model And Multiple-Based Number Conversion,” accepted and to appear in *Pattern Recognition Letters*.

[5] H. Y. Chang, “Data hiding and watermarking in color images by wavelet transforms,” *Master thesis, Department of Computer and Information Science, National Chiao Tung University, Taiwan, Republic of China*, 1999.

[6] T. K. Yen, “Image hiding by random bit replacement and frequency transformations,” *Master thesis, Department of Computer and Information Science, National Chiao Tung University, Taiwan, Republic of China*, 1998.

[7] G. Voyatzis, I. Pitas, “Applications of toral automorphisms in image watermarking,” *Proc. IEEE Internet Conf. on Image Processing* (ICIP’96), Vol. II, Lausanne, Switzerland, 16-19 September 1996, pp. 237-240.

[8] J. Fridrich, “Robust bit extraction form images,” *in Proc. IEEE ICMCS’99 Conf.* Florence, Italy, June 7-11, 1999.

[9] W. Bender, N. Morimoto, and D. Gruhl, "Method and apparatus for data hiding in images," U. S. Patent, No. 5689587, 1997.

[10] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," *in*

*Proc. IEEE Nonlinear Signal and Image Processing Workshop*, Thessaloniki, Greece, 1995, pp. 452-455.

[11] C. T. Hsu and J. L. Wu, "DCT-Based watermarking for video," *IEEE Transactions on Image Processing*, vol. 8, pp. 58-68, 1999.

[12] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal Processing*, vol. 66, pp. 357-372, 1998.

[13] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[14] C. H. Kuo and C. F. Chen, "A prequantizer with the human visual effect for the DPCM," *Signal Processing: Image Communication*, vol. 8, pp. 433-442, 1996.

[15] D. Stinson, Cryptography Theory and Practice, CRC Press, Boca Raton, 1995.

[16] S. Walton, "Information authentication for a slippery new age," Dr. Dobbs Journal, vol. 20, no. 4, pp. 18-26, April 1995.

[17] R. van Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," *Proceeding of the IEEE International Conference on Image Processing*, vol. 2, pp. 86-90, Austion, Texas, November 1994.

[18] P. W. Wong, "A public key watermark for image verification and authentication," in *Proc. IEEE International Conference on Image Processing*, vol. II, 1998, pp. 455-459.

[19] D. C. Wu and W. H. Tsai, "A Method for Creating Perceptually Based Fragile Watermarks for Digital Image Verification," submitted to *IEEE Transactions On Multimedia*.

[20] J. Fridrich, "Image watermarking for tamper detection," in *Proc. IEEE International Conference on Image Processing*, vol. II, 1998, pp. 404-408.

[21] M. Wu and B. Liu, "Watermarking for image authentication," *in Proc. IEEE International Conference on Image Processing*, vol. II, pp. 437-441, Chicago, Illinois, October 1998.

[22] D. Kundur and D. Hanzinakos, "Towards a telltale watermarking technique for tamper-proofing," *in Proc. IEEE International Conference on Image Processing*, vol. 2, pp. 409-413, Chicago, Illinois, October 1998.