A New Method for Copyright and Integrity Protection for Bitmap Images by Removable Visible Watermarks and Irremovable Invisible Watermarks*

Yu-Jen Cheng (鄭育仁) and Wen-Hsiang Tsai (蔡文祥)

Department of Computer & Information Science
National Chiao Tung University
1001 Ta Hsueh Rd., Hsinchu, Taiwan 300, R. O. C.
Tel: 886-3-5720631
Email:whtsai@cis.nctu.edu.tw

Abstract

Nowadays, digital images may be copied or tampered easily, resulting possibly in unauthorized uses or modifications of them. A new method of embedding both removable visible watermarks and irremovable invisible watermarks in BMP images is proposed to solve this problem, which is based on the use of a human visual model and the least-significant-bit replacement technique. The method can be employed to embed visible watermarks in images for direct claim of image ownership. The visible watermark is specially designed and may be removed, whenever necessary, to restore the original image, so that only the watermarked image need be kept to save storage space. On the other hand, irremovable invisible watermarks may also be embedded behind images, which may be extracted to prove the copyright of the images. Furthermore, by checking the existence of watermark signals in images, any tempering of image blocks can be detected and so the image integrity can be verified. Good experimental results prove the feasibility of the proposed method.

1. Introduction

Because of the fast development of digital processing technologies, digital images may be copied or even tampered easily, resulting in unauthorized uses, misappropriation, and misrepresentation of them. Therefore, developing methods to protect the copyright of various types of digital images and authenticate the integrity of them are desirable.

One approach for this purpose is to use digital watermarking techniques. Such techniques can be categorized into two types: visible watermarking and invisible watermarking. Many researches have been conducted on invisible watermarking [1-9]. On the contrary, studies on visible watermarking are less. However, a main advantage of creating a visible watermark on an image is that it conveys an immediate claim of the ownership of the image. It also prevents or discourages unauthorized uses of the image [10].

When using the technique of visible watermarking to prove the copyright of an image, a user has to keep the original image and the

* This work was supported partially by the Ministry of Education under the Project of Excellency No. 90-E-FA04-1-4.

corresponding watermarked one, which are called the *cover image* and the *stego-image*, respectively, in this study. It so requires a double amount of storage to keep the cover image and its stego-version. This results in a waste of storage space. Consequently, a type of *removable* visible watermark is desired. After embedding such a type of watermark in an image, a user only has to keep the resulting stego-image, instead of saving the original image as well, because the latter may now be available as the result of removing the visible watermark from the stego-image.

In this study, a method capable of embedding a visible watermark into a BMP image and removing it to restore the original image is proposed. In addition, irremovable invisible watermarks may also be embedded into images by the proposed method. By checking the existence of such watermarks, indirect copyright protection may be achieved and the integrity of the image may also be verified. The method is based on the use of a human visual model as well as the technique of least-significant bit replacement. Good experimental results prove the feasibility of the proposed method.

In the remainder of this section, a review of the properties of the BMP image format is given first. Then, the human visual model adopted in this study for watermarking is described. And in the remainder of this paper, the proposed processes of embedding and extracting watermarks in BMP images for copyright proving and integrity authentication are then described. Some experimental results are also given. Conclusions are given finally.

A. Properties of BMP Images

BMP images are of a kind of bitmap format, that is, the pixels in a BMP image are saved one after another sequentially in a bit-mapped way. In a full-color BMP image, every pixel of the image is stored in the (R, G, B) mode, where R, G, and B respectively represent the red, green, and blue channels of the image pixel. Each component value of the R, G, and B channels (called an R, G, or B channel value in the sequel) is an integer between 0 and 255, and can be expressed and stored in a byte. Therefore, three bytes are required to store a BMP image pixel.

The size of a BMP image is usually larger than that of an image of other formats because of its uncompressed innate characteristic --- it stores each pixel in full color without any loss. However, it has a primary advantage, that is, it yields high image quality, and is so especially good for keeping images that include sophisticated contents. An appropriate application of BMP images is to use them for the archiving purpose in digital libraries. In this study, we concentrate on the investigation of watermarking techniques for BMP images.

B. Review of Employed Human Visual Model for Image Watermarking and Authentication

A human visual model proposed in [11] and modified in [12] is used in this study for embedding watermarks. The use of the model aims to guarantee that the modification of the content of a cover image is imperceptible. We give a brief review of the model below.

Fig. 1 shows an example of a 3×3 image block, with the eight surrounding pixels regarded as the background of the central pixel. The adopted human visual model takes the standard deviation s of the eight surround pixels as a

parameter and classifies 3×3 image blocks into four classes, from smooth areas to edge areas. A *contrast function* of the central pixel is then defined in the following way. First, quantize the gray value range into n equal levels. Then, take the gray value g of the central pixel as an input to the function, and the quantization level, say R, in which g falls as output. Denote the two boundary values of the range R by $g_{\min}$ and $g_{\max}$, which represent respectively the lower bound and the upper bound of R. The human visual model that we adopt says that any gray value between $g_{\min}$ and $g_{\max}$ will have the same sensitivity to human vision under any background (the eight surrounding pixels in a 3×3 image block here) with the same standard deviation s. The number of the quantization levels for the model may be specified by a criterion below:

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

129	138	136
129	138	136
129	138	136

Figure 1. A 3×3 image block and its gray values.

In the example shown in Fig. 1, the standard deviation s of the eight surrounding pixels is about 3.95. The contrast function values for the central pixel will so be equally quantized into 16 levels according to the criterion above. The gray value 138 of the central pixel falls within the quantization level range from 128 to 143. It means that any gray value between 128 and 143 can be used to replace that of the central pixel without making perceptible effects to human eyes.

2. Proposed Copyright and Integrity Protection Method by Watermarking

The proposed method for embedding a removable visible watermark and an irremovable invisible watermark in a BMP image based on the previously-mentioned human visual model and a least-significant-bit replacement technique will be described in this section. In Section A, the proposed method of embedding irremovable invisible watermarks by LSB replacement is introduced. In Section B, the proposed method of embedding irremovable invisible watermarks by the use of the human visual model is described. In Section C, the proposed method of embedded visible watermarks is described. In Section D, the proposed method of authentication of image integrity by extracting watermarks is explained. In Section E, the proposed method for recovering original images by removal of watermarks is introduced. In Section F, the overall process of the proposed methods is presented.

A. Embedding of Irremovable Invisible Watermarks by LSB Replacement

In the proposed method, we use LSB's in the B channel to indicate those pixels in which visible watermark signals are embedded. The replacement of LSB's will not cause much distortion of the input image. We replace only the least-significant bit of a pixel, with 1 as a visible watermark signal and 0 as a non-watermark signal. For example, assume that a pixel used to embed a watermark signal has a pixel value of $(10011100)_2$. In order to mark the

watermark signal embedded in this pixel, the pixel value becomes $(10011101)_2$, where the LSB 0 is replaced by the value 1.

B. Embedding of Irremovable Invisible Watermarks by A Human Visual Model

We use the human visual model mentioned previously in the proposed method to embed watermarks in image blocks. The human visual model guarantees that the modification of the cover image is not perceptible by human eyes. In the embedding process, we use the human visual model to separate image blocks into two groups, namely, *watermarked blocks*, and *un-watermarked ones*. In the watermark extraction process, we can correctly categorize all image blocks into these two groups. And any image block that does not belong to these two groups is thought as a *tampered block*. Therefore, with the help of the human visual model we can extract the watermark and authenticate the integrity of the image in the mean time. Furthermore, we can remove the embedded watermark, too.

More specifically, in the proposed method we use the G channel of the image to embed irremovable watermark signals. Two constants α and β are used to distinguish watermarked blocks from un-watermarked ones. We mark a block in which a visible watermark signal is embedded by replacing the gray value of the central pixel of the block with $g_{\min} + \alpha$, where $g_{\min} + \alpha \le g_{\max}$ and $g_{\min}$ and $g_{\max}$ are the lower and the upper bounds of the quantization level R yielded by the contrast function mentioned previously with the gray value of the central block pixel as input. And we identify a block in which no visible watermark is embedded by replacing the central pixel's value by $g_{\min} + \beta$, where $g_{\min} + \beta \le g_{\max}$. In short, we take $g_{\min} + \alpha$ and $g_{\min} + \beta$ as irremovable invisible watermark signals and embed them in the image for the purpose of marking image blocks as watermarked and un-watermarked ones, respectively.

C. Embedding of Removable Visible Watermarks by Image Color Adjustment

To create visible watermarks, we adjust the image colors in the R channels of those pixels in which visible watermark signals are embedded. Because of the adjustment, the embedded watermark can be seen, that is, it is visible. The adjustment procedure is as follows. First, the color values of both the image and the watermark are reduced according to an *embedding factor*. Then the desired *watermark color* is obtained by adding both of them together. With the help of the embedding factor, we can recover the original color from the watermark color by performing an inverse operation. The details will be described later.

D. Extraction of Watermarks for Copyright Verification and Integrity Authentication

We extract the embedded visible watermark for copyright verification by using the human visual model and the LSB replacement technique. And then we use the human visual model to authenticate the integrity of the image.

To extract the visible watermark, we check if the value of the central pixel of the G channel of a given image block is equal to $g_{\min} + \alpha$ or not. If it is, the LSB of each pixel in the block is checked in the following way to find out those pixels in which visible watermark signals were embedded: if the LSB of a pixel is equal to the value 1, it is decided that a visible watermark signal has been embedded in the pixel, and set the corresponding pixel value in a *extraction*

result image to black; otherwise, set it to white. After this process is completed, the embedded visible watermark is extracted ant put into the extraction result image. And the copyright of the original image can be proved by visual inspection of the completeness of the reconstructed watermark in the extraction result image.

On the other hand, to authenticate image integrity, we check the G channel value of the central pixel of each image block in the following way: if the central pixel value is not equal to $g_{\min} + \alpha$ or $g_{\min} + \beta$, then decide that the block has been tampered, and mark the corresponding block in the extraction result image by the black color; otherwise, mark the corresponding block to white. After checking all the image blocks, the integrity of the image can be authenticated by inspecting the extraction result image to see whether black tampered blocks exist or not.

E. Recovery of Original Images by Removal of Visible Watermarks

We utilize the embedded irremovable invisible watermark signals in the stego-image as an assisting tool to remove the visible watermark signals and get a *restored image*. First, by detecting the irremovable invisible watermark signal embedded according to the human visual model, watermarked blocks can be found. Then by detecting the LSB's in each watermarked block, each watermarked pixel can be found out and the removal of the embedded visible watermark can be started.

More specifically, in the beginning the G channel value of the central pixel of each block in a given stego-image is extracted. If the extracted value is equal to $g_{\min} + \alpha$, it is decided that watermark signals have been embedded in the block. Then the LSB value of the B channel of each pixel is checked. If the value is equal to 1, then it is decided that a visible watermark signal exists in the R channel of the pixel and a signal removal process is started; otherwise, let the R channel value of the pixel be unchanged. On the other hand, if the central pixel value of a given stego-image block is equal to $g_{\min} + \beta$, it means that no watermark signal is embedded in the block, and we let the block be unchanged. Finally, if the central pixel value is equal neither to $g_{\min} + \alpha$ nor to $g_{\min} + \beta$, then the block is decided to be tampered and is marked black to indicate so. After checking all the blocks of the given image, a restored image is obtained with the tampered areas being marked.

3. Detailed Processes of Proposed Method for Copyright and Integrity Protection

In this section, the details of all the proposed processes of watermark embedding, extraction, and authentication are described. In the beginning, we define some symbols that will be used in the sequel. Let C be a cover image and S a stego-image both of size $M \times N$. We use $c_{x,y}$ to indicate a 3×3 image block of C with (x, y) representing the coordinates of the block in the cover image, satisfying the conditions $0 \le x \le \left\lfloor \frac{M}{3} \right\rfloor - 1$ and $0 \le y \le \left\lfloor \frac{N}{3} \right\rfloor - 1$. Fig. 2 shows the coordinates of blocks in a cover image. And we use the symbol p_h to denote a pixel in a 3×3 image block, and the symbols r_h, g_h, and b_h with $1 \le h \le 9$ to represent respectively the three color values of the pixel located at h. Fig. 3 shows an example of a 3×3 image block. We use p_5 to represent the central pixel of the block. Let W be a binary watermark of size $E \times F$ that will be embedded in C. Then we use $w_{i,j}$ to represent a

3×3 binary watermark block, where (i, j) represent the coordinates of the block with $0 \le i \le \lfloor \frac{E}{3} \rfloor - 1$ and $0 \le j \le \lfloor \frac{F}{3} \rfloor - 1$. Fig. 2 shows an example. We use wp_h to indicate a pixel value in a 3×3 binary watermark block, where $1 \le h \le 9$. If a watermark pixel is black, then the value of wp_h is set to 255; otherwise, to 0. On the other hand, the embedding factor k is a user-defined constant, where $0 \le k \le 1$. Two constants α and β are also used in the proposed method.

(0,0)	(1,0)	(2,0)	…
(0,1)	(1,1)	(2,1)	…
(0,2)	(1,2)	(2,2)	…
(0,3)	(1,3)	(2,3)	…
⋮	⋮	⋮	⋱

Figure 2 Coordinates of 3×3 image blocks in an image.

1	2	3
4	5	6
7	8	9

Figure 3 Locations of pixels in a 3×3 image block.

A. Process of Embedding Removable Visible Watermarks and Irremovable Invisible Watermarks

The whole process of embedding removable visible and irremovable invisible watermarks is described below.

Step 1: Divide both the cover image C and the watermark image W into non-overlapping 3×3 image blocks.

Step 2: For every 3×3 image block $c_{x,y}$, find its corresponding 3×3 watermark block $w_{x,y}$, where $0 \le x \le \lfloor \frac{E}{3} \rfloor - 1$ and $0 \le y \le \lfloor \frac{F}{3} \rfloor - 1$.

Step 3: In each 3×3 image block $c_{x,y}$, in which we need to embed the watermark, compute the standard deviation s of all the pixel values of the G channel of the block and find $g_{\min}$ and $g_{\max}$ based on the contrast function out of the human visual model with s as input. Replace the value g_5 of the central pixel of the block with $g_{\min} + \alpha$.

Step 4: For each black watermark pixel wp_h, which needs to be embedded, replace the LSB of the value of b_h of the corresponding pixel with the value 1. Calculate $r_h' = (1 - k) \times r_h + k \times wp_h$, and replace r_h with r_h'. For each of the other watermark pixels that are white and need not be embedded, replace the LSB of the corresponding pixel with the value 0.

Step 5: In each un-watermarked 3×3 image block, for which there exists no black watermark pixel in its corresponding 3×3 watermark block, compute the standard deviation s of all the pixel values of the G channel and find g_{min} and g_{max} according s using the contrast function of the human visual model. Replace the value of the central pixel g_5 of the un-watermarked block with the value $g_{\min} + \beta$. Take the watermarked image block as a stego-image block $s_{x,y}$.

Step 6: For each of the other 3×3 image block $c_{i,j}$, where $\lfloor \frac{E}{3} \rfloor \le i \le \lfloor \frac{M}{3} \rfloor - 1$ and

$\lfloor \frac{F}{3} \rfloor \le j \le \lfloor \frac{N}{3} \rfloor - 1$, calculate the standard deviation s of the block and find g_{min} and g_{max} using the contrast function of the human visual model. Replace the value of the central pixel g_5 of the block is by $g_{\min} + \beta$. Take the processed image block as a stego-image block $s_{i,j}$.

After all the steps are executed, a stego-image is obtained.

B. Process of Authentication of Image Integrity

Let A be the extraction result image of size $M \times N$, corresponding to a given input image S. The proposed process for image integrity authentication is described below.

Step 1: Divide the input image S into non-overlapping 3×3 image blocks, and denote each of them by $s_{x,y}$.

Step 2.: For each 3×3 image block $s_{x,y}$, calculate the standard deviation s of all the G channel values of the pixels of $s_{x,y}$ and find the corresponding g_{min} according to the contrast function of the human visual model.

Step 3: If the central pixel g_5 of $s_{x,y}$ has a G channel value equal to $g_{\min} + \alpha$, it means that visible watermark signals have been embedded in the image block $s_{x,y}$. Check the LSB value b_q of the B channel value of each pixel p_q in $s_{x,y}$. If b_q is equal to 1, then decide that a watermark signal has been embedded in this pixel and mark the corresponding pixel in the extraction result image A as black; otherwise, mark the corresponding pixel in A as white.

Step 4: If the value of the central pixel g_5 of $s_{x,y}$ is equal to $g_{\min} + \beta$, it means that no watermark is embedded in the block, and mark all the corresponding pixels of the image block in the extraction result image A as white.

Step 5: If the value of the central pixel g_5 is equal to neither $g_{\min} + \alpha$ nor $g_{\min} + \beta$, mark the corresponding block in the extraction result image A as a tampered block (also as black).

Step 6: Perform Steps 2 through 5 until all image blocks are processed. The final result is a complete extraction result image A.

C. Process of Recovery of Original Image

Let R be the restored image of size $M \times N$, corresponding to a given input image S. The proposed process of removing visible watermarks is described in the following.

Step 1: Divide the input image S into non-overlapping 3×3 image blocks, and denote each of them by $s_{x,y}$.

Step 2: For each 3×3 image block $s_{x,y}$, compute the standard deviation s of the G channel values of all the pixels of $s_{x,y}$ to find the corresponding g_{min} according to the contrast function of the human visual model.

Step 3: If the value of the central pixel g_5 of $s_{x,y}$ is equal to $g_{\min} + \alpha$, it means that visible watermark signals have been embedded in $s_{x,y}$. Then check the LSB of the B channel value b_q of each pixel p_q of $s_{x,y}$ to find watermarked pixels in the following way: if b_q is equal to 1, decide that p_q is a watermarked pixel and calculate the value $r_q' = (r_q - k \times wp)/(1 - k)$ to replace the original gray

value r_q of p_q, where wp is 255. Otherwise, if b_q is equal to 0, let r_q be unchanged.

Step 4: If the value of the central pixel g_5 of $s_{x,y}$ is equal to $g_{\min} + \beta$, it means that no watermark is embedded in the image block. Let the image block be unchanged.

Step 5: If the value of the central pixel g_5 of is equal to neither $g_{\min} + \alpha$ nor $g_{\min} + \beta$, then mark the image block $s_{x,y}$ as a tampered one by changing the each original pixel value r_q in the block to be $r_q' = (r_q - k \times wp)/(1 - k)$. And then take all the new pixel values of the block into the corresponding pixels of the restored image R.

Step 6: Perform Steps 2 through 5 until all image blocks are processed. The final result is a restored image R.

In Step 5 above, changing the value r_q into the specific value $r_q' = (r_q - k \times wp)/(1 - k)$ is just one possible way taken in this study. Other proper choices of the new value r_q' may also be taken as long as the resulting marking effect of tampered blocks is visually obvious in the restored image R.

4. Experimental Results

In one of our experiments, an image of size 256×256 is used as the visible watermark, which is shown in Fig. 4. Figs. 5(a), (b), and (c) show three cover images all with the size of 512×512. And Figs. 5(d), (e), and (f) show the three resulting stego-images after the proposed watermark embedding process was performed with the embedding factor k = 0.4. Fig. 6(a) shows a stego-image of Fig. 5(a). Fig. 6(b) shows a tampered image of Fig 5(d). Fig. 6(c) shows a tampered image of Fig 5 (f). Figs. 6(d) and (e) show the authentication results (i.e., the extraction result images) of Figs. 6(a) and (b), respectively. Fig. 6 (f) shows the restored image of Fig. 6 (c) with the tampered areas being located and marked in nearly blue colors. Figs. 7(a) through (c) show the restored images of Figs. 5(d) through (f), respectively. The PSNR values of the restored images are shown in Table 1. These values show that the restored image quality is acceptable.

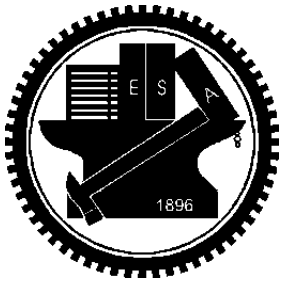


Figure 4 A watermark image of size 256×256.

Table 1 The PSNR values of the images after removing the embedded visible watermark.

	Lena	Baboon	Jet
PSNR	45.1	44.0	47.0

5. Conclusions

In this paper, a new method for protecting the copyright and verifying the integrity of BMP images is proposed. Visible watermarks are embedded in cover images to prove the copyright and the ownership of the cover images. And the embedded visible watermark can be removed from the stego-images to restore the original images. This will save image storage space because only the stego-images need be saved now. On the other hand, to authenticate

the integrity of the cover image, invisible watermarks are also embedded by the LSB replacement technique to mark the watermarked pixels of the cover image. A human visual model is adopted to embed a fragile watermark. With the help of the fragile watermark, tampered areas within the stego-image may be detected and located, so achieving the authentication of the image integrity.

References

[1] H. Y. Chang, "Data hiding and watermarking in color images by wavelet transforms," *Technical Report, Department of Computer and Information Science, National Chiao Tung University, Taiwan, Republic of China*, 1999.

[2] 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.

[3] J. Fridrich, "Robust bit extraction form images," *Proc. IEEE ICMCS'99 Conf.*, Florence, Italy, June 7-11, 1999.

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

[5] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," *Proc. IEEE Nonlinear Signal and Image Processing Workshop*, Thessaloniki, Greece, 1995, pp. 452-455.

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

[7] 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.

[8] 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.

[9] 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.

[10] A. R. Rao, F. C. Mintzer, G. W. Braudaway, and M. Yeung, "Digital Watermarking for High-quality Imaging," *Proc. IEEE First Workshop on Multimedia Signal Processing*, Princeton, NJ, USA, June 1997, pp. 357-364.

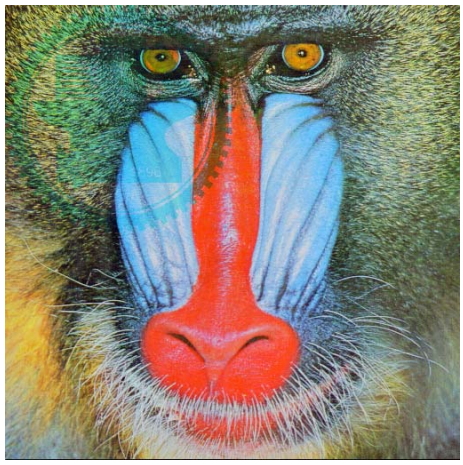
[11] C. H. Kuo and C. F. Chen, "A prequantizer with the human visual effect for the DPCM," *Signal Processing: Image Communication*, vol. 8, pp. 433-442, 1996.

[12] 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.*

(a)

(d)

(b)



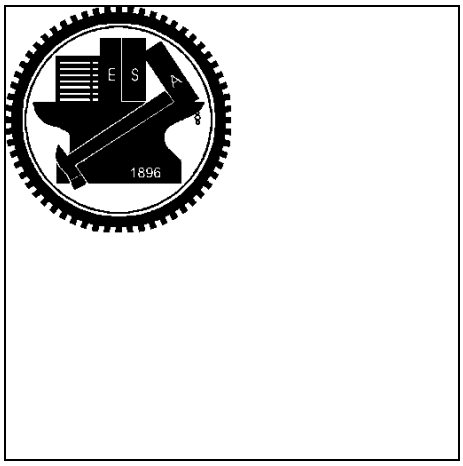
(e)

(c)

(f)

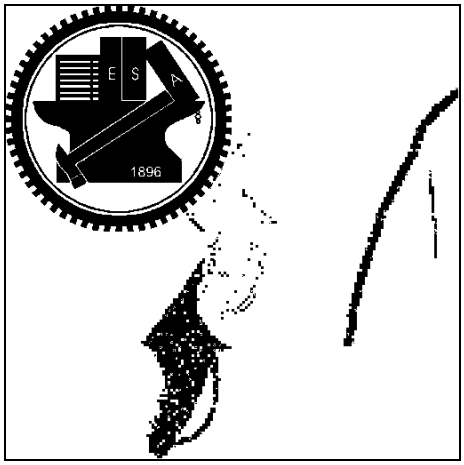
Figure 5 The cover images, and stego-images with the visible watermark of Fig. 4. (a) Cover image “Lena”. (b) Cover image “Baboon”. (d) Cover image “Jet”. (d) - (f) Stego-images after embedding visible watermark Fig. 4.

(a)



(d)

(b)



(e)

(c)

(f)

Figure 6 Some tampered images and its authentication results. (a) Stego-image without tampering. (b) Tampered image “Lena”. (c) Tampered image “Jet”. (d) & (e) the authentication results. (f) Restored image.

(a)

(c)

(b)

Figure 7 The restored images of Figs. 5(d) through (f). (a) Restored image “Lena”. (b) Restored image “Baboon”. (c) Restored image “Jet”.