Chrysochos E., Fotopoulos V., Skodras A., Xenos M., "*Reversible Image Watermarking Based on Histogram Modification*", 11th Panhellenic Conference on Informatics with international participation (PCI 2007), Vol. B, pp. 93-104, 18-20 May 2007, Patras, Greece.

# Reversible Image Watermarking Based on Histogram Modification

E. Chrysochos, V. Fotopoulos, A. N. Skodras, M. Xenos
Digital Systems & Media Computing Laboratory,
School of Science and Technology, Hellenic Open University,
13-15 Tsamadou st., GR-26222, Patras, Greece
{e.chrysochos, vfotop1, skodras, xenos}@eap.gr

**Abstract**

In this paper, a new reversible watermarking scheme resistant to geometrical attacks is presented. The proposed scheme does not need the original image for extracting the watermark, and induces not noticeable distortion during the watermarking procedure. The embedding algorithm has low computational complexity, can be applied to very small images (down to 16 x 16), and provides capabilities of multicasting. The watermarked images show robustness against geometrical attacks like rotation, flipping, translation, aspect ratio changes and resizing, warping, shifting, drawing, scattered tiles, shaking as well as their combinations.

**Keywords:** blind, reversible, robust watermarking, histogram modification, geometrical attacks

## *1. Introduction*

During the last decade we have witnessed the domination of digital media. As opposed to analogue, digital data are in many cases easier to manipulate, while the result can be reproduced infinitely without any loss of quality. The new digital reality provides users with many accommodations like high quality, manipulation of the context, creation of perfect duplicates, streaming over the internet etc. Nevertheless these technologies in combination with the World Wide Web enable the perfect copying and distribution of copyrighted material anywhere in the world with practically no cost. Therefore a significant problem of non authorized copying and distribution of digital media is raised [1]. Also in certain cases the problem of authenticity and reliability is raised (like in medical or military implementations). Digital Watermarking is called to cope with some of these issues.

Movie and record industries, as well as media industry in general, suffer huge economic losses from piracy. Consequently there is an increasing interest in recent years in the area of Digital Watermarking. [2]. Digital Image Watermarking stands

for embedding a signature signal, called 'watermark', in a digital image, in order to prove ownership, or check authenticity or integrity of a certain image. A watermarked image can sustain various attacks (malicious or unintended) which ultimately could destroy our ability to perceive the watermark. When the watermark is still perceivable after some attacks, the process is referred as robust watermarking [3]. Robust watermarking is usually used for copyright control. In the opposite, fragile watermarking is the case where the watermark is embedded to an image in such a way, that the slightest alteration of the image, due to an attack, would make the watermark unperceivable [4, 5, 6, 7]. Fragile watermarking is usually used for authenticity check, or integrity examination.

At present most watermarking schemes perform poorly against geometrical attacks [8]. The most common geometrical attacks are rotation, flipping, translation, aspect ratio changes, resizing and cropping. In many cases in order to handle geometrical attacks, watermarking schemes employ several synchronization methods. These methods usually try to identify the geometrical distortions and invert them, before the watermark detector is applied. The identification of the geometrical distortions is achieved by examining a registration pattern embedded along with the watermark in the host image [9, 10]. However the addition of the registration pattern to the data-carrying watermark reduces the fidelity of the watermarked image, as well as the scheme's capacity. Another weakness of this approach is that usually all the watermarked images carry the same registration watermark. Therefore it is easier to discern the registration watermark by collusion attempts. Once found, the registration pattern could be removed from all the watermarked images, thus restricting the invertibility of any geometric distortions. Additionally these methods increase computational time substantially and in some cases perform poorly.

There are also watermarking schemes that try to achieve robustness against geometrical attacks, using transformations, invariant to some attacks, and correlation functions like [11] and [12]. Although such schemes show good results with regard to robustness, they require high computational complexity during embedding as well as during extracting the watermark.

In this paper, a novel watermarking scheme of low computational cost is proposed. This scheme performs excellent against most frequently used geometrical attacks. The rest of this paper is organized as follows. In section 2, the proposed reversible watermarking scheme based on histogram modification is described in detail. Experimental results are presented in section 3, while conclusions are drawn in section 4.

## *2. Proposed Image Watermarking Scheme*

### *2.1 Features of the Proposed Scheme*

The proposed watermarking scheme has the following features:

- Reversible; the watermarked image can be fully restored to its original status.
- Blind; in order to detect the watermark only the watermarked image is needed.
- Asymmetric; a public key is used for detecting the watermark and a private key is used for restoring the watermarked image.
- Robust against geometrical attacks like rotation, flipping, translation, aspect ratio changes and resizing, warping, shifting, drawing, scattered tiles as well as their combinations.
- Multicast; a certain watermark can be embedded several times to increase robustness.
- Low computational cost.
- Applicable to very small images (down to 16 x 16).
- Applicable to color images.
- Good watermarked image quality.

The basic principle of this scheme is based on the permutation of histogram bins, which are chosen in couples, according to a specific rule. For embedding the watermark a key is needed. This is a real number that specifies the area where the watermark is to be embedded. This key is also necessary for the detection and extraction of the watermark. Therefore it is considered as public key. A second key, which is referred to, as private key, is used for the full restoration of the image.

### *2.2 Watermark Embedding*

The most important parameter needed, in order to embed the watermark into the host image, is the public key. This key (as mentioned above) is a real number that determines the area where the watermark is to be embedded. Its integer part (*start*) indicates the point of the histogram, where the embedding procedure will start choosing histogram bin couples. Its decimal part, multiplied by ten, defines the minimum distance, two histogram bins of a couple may have. We will refer to this distance as *step*.

$$start = \text{public\_key div } 1$$

$$step = 10*(\text{public\_key mod } 1)$$

The steps, of the embedding algorithm, in order to embed a watermark in a grayscale image are the following:

a. The histogram of the host image is computed
b. *start* and *step* are calculated with respect to the public key.

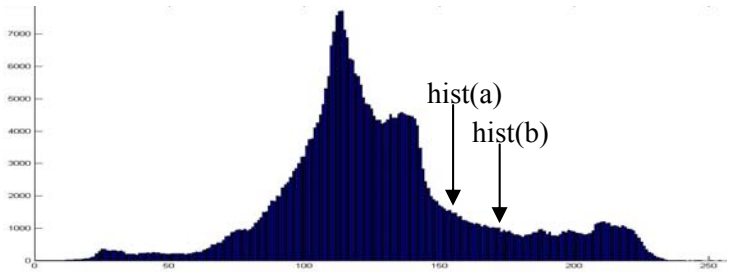



***Figure 1**. Host Image Histogram and corresponing couple (a,b)*

c. The first couple (a,b) of the histogram bins is chosen according to *start* and *step*. If the corresponding values of the histogram hist(a) and hist(b) are equal, we reject this couple and we continue with the next one.

d. For each couple (a,b) and each bit (w) of the watermark respectively, the following rule is applied. If w equals zero then the histogram values (hist(a), hist(b)) should be in ascending order. In the opposite case, i.e. when w equals one, the histogram values should be in descending order.

$$w=0 \rightarrow hist(a)<hist(b)$$
$$w=1 \rightarrow hist(a)>hist(b)$$

If the values of a couple are not in the right order according to this rule, then they are swapped, in order to follow the rule. When two values of the histogram are swapped, we ensure that the value of the corresponding pixels, with luminance a and b respectively, are interchanged.

e. The next couple (a,b) of the histogram bins is chosen according to *start* and *step* for embedding the next bit (w) of the watermark. Steps c and d of the algorithm are repeated until all bits (w) of the watermark are embedded in the image.

f. The private key, which is necessary for the restoration of the image, is generated in accordance with the procedure watermark embedding. For each couple (a,b) of the histogram bins that are chosen, a bit (pk) of the private key is generated according to this rule: if originally hist(a) and hist(b) are in ascending order, pk equals zero. Else, if originally hist(a) and hist(b) are in descending order, pk equals zero.

$$hist(a)<hist(b) \rightarrow pk=0$$
$$hist(a)>hist(b) \rightarrow pk=1$$

In case that the algorithm reaches the end of the histogram (which corresponds to an intensity of 255), it continues from the beginning of the histogram (which

corresponds to an intensity of 0), provided that the couple (a,b) does not collide with a previously selected couple. In order to avoid artifacts in the watermarked image, the maximum distance between a and b is set to 9. Another case where artifacts could arise, is when a is at the end of the histogram, while b is at the beginning. Such a case is foreseen and prohibited.

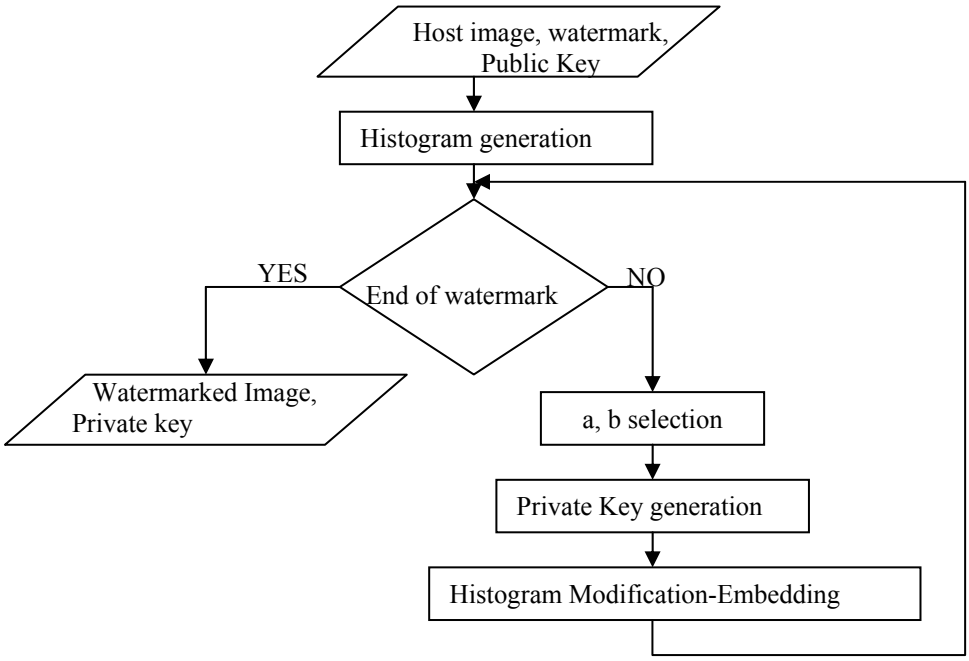



***Figure 2.*** *Embedding Algorithm*

During the watermark embedding, as we can see in figure 3, the shape of the histogram stays almost unaltered.

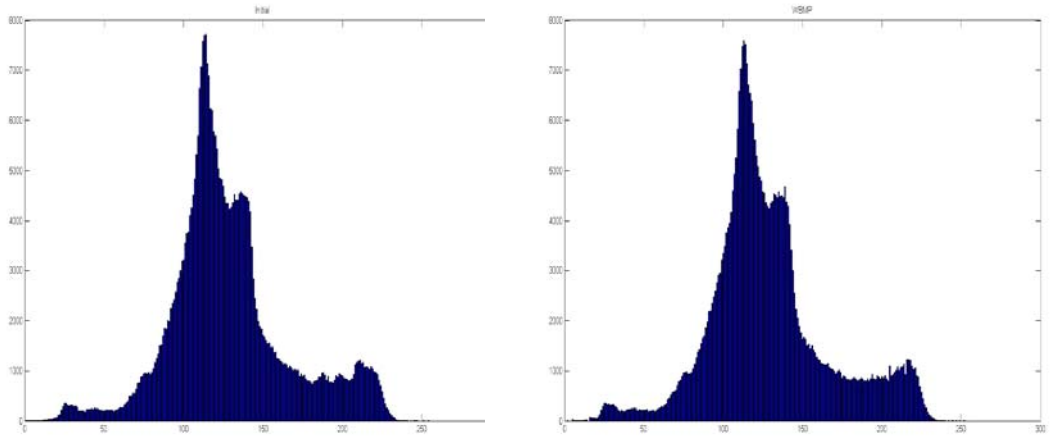


***Figure 3.*** *Histograms of the original (left) and the watermarked (right) images*

Only when the two histograms are more thoroughly examined, one can see in detail

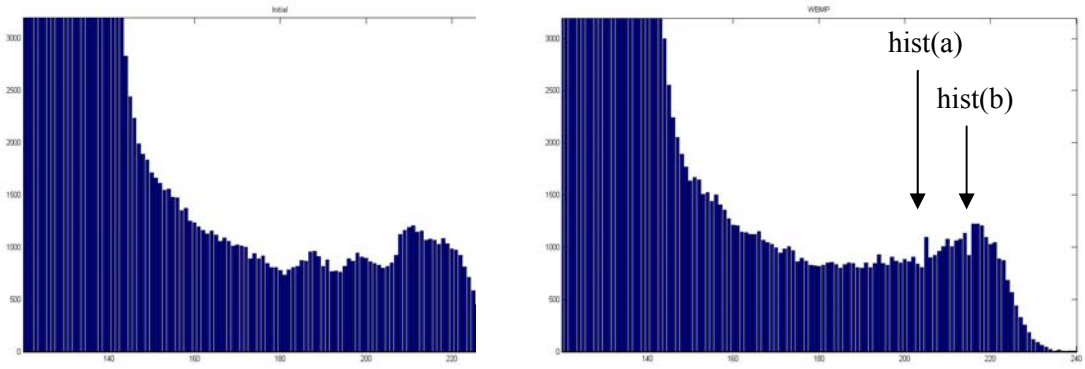



***Figure 4.*** *Close-up views of the histograms of fig.3*

the changes that are induced by the embedding algorithm, as the histogram bins are interchanged. This is shown in figure 4.

### *2.3 Watermark Extraction*

The parameters needed in order to extract the watermark from a possibly marked image, apart from the image itself, is the public key and the watermark size. The public key, as mentioned above is a real number that determines the histogram area where the watermark is embedded in. The scheme is blind and thus there is no need for the original image.

The steps, of the extracting algorithm, in order to extract the watermark out of a grayscale image are the following:

a. The histogram of the watermarked image is computed
b. *start* and *step* are calculated with respect to the public key.
c. The first couple (a,b) of the histogram bins is chosen according to *start* and *step*. If the corresponding values of the histogram hist(a) and hist(b) are equal, this couple is rejected and the process continues with the next one.
d. Each couple (a,b) corresponds to a single bit (w) of the watermark. The following rule is applied. If the histogram values (hist(a), hist(b)) are in ascending order w equals zero. In the opposite case, where histogram values are in descending order w equals one.

$$\text{hist}(a)<\text{hist}(b) \rightarrow w=0$$
$$\text{hist}(a)>\text{hist}(b) \rightarrow w=1$$

e. The next couple (a, b) of the histogram bins is chosen according to *start* and *step* for extracting the next bit (w) of the watermark. Steps c and d of the

algorithm are repeated until all the bits (w) of the watermark are extracted. It is crucial for the extracting process, to choose the same couples (a, b), that were chosen during the embedding process. Therefore the choice of the couples follows exactly the same rules with the embedding algorithm.

The process of extracting the watermark can be successful only if the couples that are chosen for extraction are exactly the same with those, chosen for embedding.

### *2.4 Restoration of Watermarked Images*

In order to restore the watermarked image to its original form, both the private and the public keys are needed. The private key is the key that has been created during the embedding process.

The steps of the restoring algorithm, in order to retrieve the original image, are the following:

a. The histogram of the watermarked image is computed
b. *start* and *step* are calculated with respect to the public key.
c. The first couple (a,b) of the histogram bins is chosen according to *start* and *step*. If the corresponding values of the histogram hist(a) and hist(b) are equal, this couple is rejected and the algorithm proceeds to the next one.
d. For each couple (a,b) and each bit (pk) of the private key respectively, the following rule is applied. If pk equals zero then the histogram values (hist(a), hist(b)) should be in ascending order. In the opposite case, where pk equals one, the histogram values should be in descending order.

$$pk=0 \rightarrow hist(a)<hist(b)$$
$$pk=1 \rightarrow hist(a)>hist(b)$$

If the values of a couple are not in the right order according to this rule, then they are swapped, in order to follow the rule. When two values of the histogram are swapped, the intensity values of the corresponding pixels are interchanged.

e. The next couple (a,b) of the histogram bins is chosen according to *start* and *step*. Steps c and d of the algorithm are repeated until all the bits (pk) of the private key are examined with respect to the histogram. It is crucial for the restoring process to choose the same couples (a, b), that were chosen during the embedding process. Therefore the choice of the couples follows the exact same rules with the embedding algorithm.

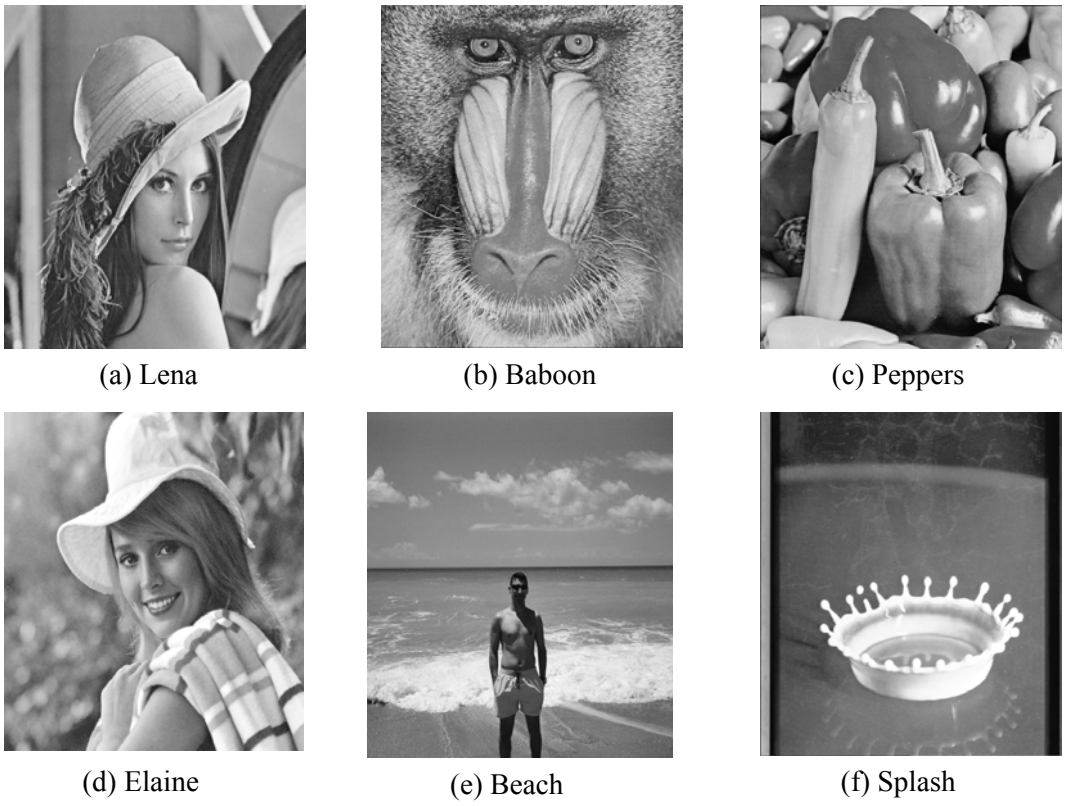
## *3. Experimental results*

The watermarking algorithm that was described in section 2.2, could be also applied for the case of color pictures. The only difference is that instead of gray scale

intensity values, it should be applied to the color components, RGB, or YCbCr respectively. In this way the watermark will be embedded three times, thus achieving improved robustness. The robustness in geometrical attacks is increased, as a change in a pixel affects different bins of each component's histogram, thus it is less probable that all three watermarks are affected in the same way. Furthermore, robustness may increase more by embedding a symmetrical watermark, in a way that allows integrity check, as well. So, if the extracted watermark follows a given symmetry, it is ensured that the watermark is intact. On the other hand, if increased capacity is of prime concern, a three times larger watermark can be embedded partially in each color component.

The maximum capacity of this scheme is rather low, namely 128 bits, but it may rise to 384 bits, if we use three color components. It has the advantage, though, that it can be applied to very small images (down to 16 x 16), with reduced capacity. The scheme may provide up to 2304 different public keys (256 different values for *start**9 different values for *step*) for gray scale images and 12.230.590.464 different public keys (2304^3) for color images.

The experimental results of the proposed method, for the images of figure 5, are shown in Tables 1 and 2.



(a) Lena (b) Baboon (c) Peppers

(d) Elaine (e) Beach (f) Splash

***Figure 5.*** *Original Images*

***Table 1.*** *Experimental results for different images and embedded bits*

| Images | Resolution | Pixel Depth | PSNR(dB) | Embedded Bits | Public key | Distance |
|---|---|---|---|---|---|---|
| Beach | 512 x 512 | 24 | 53.463 | 120 x 3 | 100.1 | 1 |
| Beach | 512 x 512 | 24 | 45.754 | 50 x 3 | 70.4 | 4 |
| Peppers | 512 x 512 | 24 | 55.185 | 100 x 3 | 200.1 | 1 |
| Splash | 512 x 512 | 24 | 54.432 | 110 x 3 | 24.1 | 1 |
| Baboon | 512 x 512 | 24 | 54.120 | 120 x 3 | 250.1 | 1 |
| Lena | 512 x 512 | 24 | 53.102 | 100 x 3 | 50.1 | 1 |
| Lena | 512 x 512 | 24 | 48.210 | 50 x 3 | 21.3 | 3 |
| Lena | 512 x 512 | 24 | 43.935 | 30 x 3 | 19.6 | 6 |
| Lena | 512 x 512 | 24 | 41.270 | 20 x 3 | 19.9 | 9 |
| Lena | 200 x 200 | 24 | 54.880 | 80 x 3 | 17.1 | 1 |
| Lena | 200 x 200 | 24 | 49.752 | 60 x 3 | 17.2 | 2 |
| Elaine | 512 x 512 | 8 | 53.670 | 100 x 1 | 30.1 | 1 |
| Elaine | 512 x 512 | 8 | 49.296 | 50 x 1 | 24.3 | 3 |

***Table 2.*** *Experimental results of robustness with regard to distance parameter*

| Attacks | Robustness over distance |
|---|---|
| Flipping | Any |
| Rotation ($90^0$, $180^0$, $270^0$) | Any |
| Rotation (arbitrary) | Over 5 |
| Upsizing | Any |
| Downsizing | Over 5 |
| Aspect ratio changing (increasing) | Any |
| Aspect ratio changing (decreasing) | Over 5 |
| Cropping (80%) | Over 5 |
| Shifting (80%) | Over 5 |
| Warping | Over 5 |
| Scattered tiles | Any |
| Shaking | Over 5 |
| Translation | Any |
| Drawing | Over3 |

The robustness of the watermark depends on the distance parameter used during the embedding (Table 2). As the distance between the bins of a couple grows, the watermark becomes more robust. This is expected as the stronger the attack is, the more it changes the histogram. The disadvantage is that while the distance grows, the capacity of the scheme reduces. This could be balanced if the embedding algorithm was allowed to execute more than one pass through the histogram values, as long as the, already selected couples (a, b), stay intact. In this way the capacity of the scheme, given a distance parameter over 5, would rise to the capacity of the scheme with distance parameter 1, namely 128 bits.

The scheme shows 100% robustness against some attacks, regardless of the distance parameter. Such attacks are flipping, rotation ($90^0$, $180^0$, $270^0$), translation, upsizing, increasing aspect ratio and scattered tiles, as well as their combinations. Against some other attacks the parameter of distance is crucial. Such attacks are arbitrary rotation, cropping, shifting, warping, shaking, drawing, downsizing and decreasing aspect ratio, as shown in Table 2. Some of the attacks to the watermarked images are shown in figure 6.

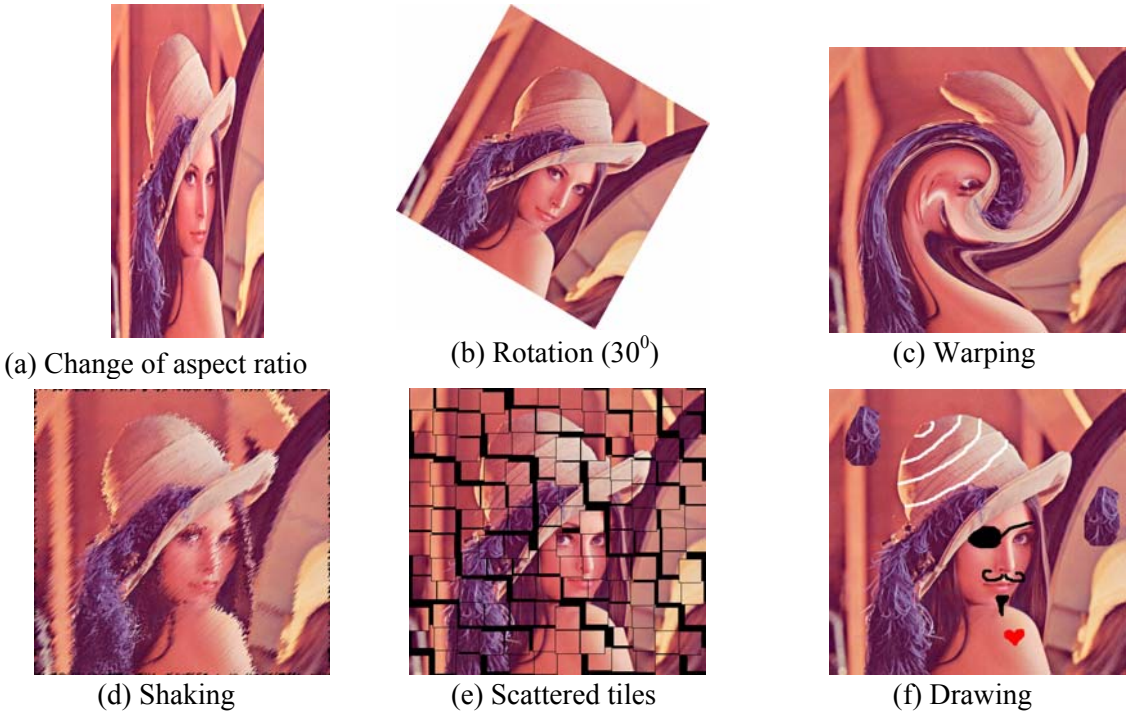
The proposed algorithm can also work with very small images, down to 16 x 16. Naturally the provided capacity, for each picture, is lower, 30-50 bits. This could work effectively against the mosaic attack given the proper synchronization. By splitting a 200 x 200 gray scale Lena, in 256 smaller images, we managed to embed 8.4 Kbits of information. The same was applied to a color image, where we had a total of 25Kbits of embedded information or 0.21 bits per pixel. The disadvantage of this method is that we loose in robustness, as synchronization of the segmentation process is crucial.

Most watermarking schemes that pursue robustness to geometrical attacks, they achieve it, either by having extremely reduced capacity [13, 14], or by having high computational cost [15, 16]. The proposed watermarking scheme combines qualities like robustness to geometrical attacks, high capacity and low computational cost.

## *4. Conclusions*

A reversible watermarking scheme for images has been proposed, based on modification of the image's histogram. The proposed scheme is 100% robust against some geometrical attacks like flipping, rotation ($90^0$, $180^0$, $270^0$), translation, upsizing, increasing aspect ratio and scattered tiles, as well as their combinations. It also shows robustness against arbitrary rotation, cropping, shifting, warping, shaking, drawing, downsizing and decreasing aspect ratio. Another advantage of the proposed embedding algorithm is that it can be applied to very small images, down to 16 x 16. Nevertheless the proposed scheme is not robust against attacks like low pass filtering. Our future work is to combine the proposed algorithm with a DCT embedding

algorithm to create a hybrid system that will be robust to a larger variety of attacks while maintaining low computational cost.



(a) Change of aspect ratio (b) Rotation ($30^0$) (c) Warping

(d) Shaking (e) Scattered tiles (f) Drawing

***Figure 6*** *Attacks against watermarked Lena image*

## *Acknowledgements*

This work was funded by the European Union - European Social Fund (75%), the Greek Government - Ministry of Development - General Secretariat of Research and Technology (25%) and the Private Sector in the frames of the European Competitiveness Programme (Third Community Support Framework - Measure 8.3 - programme ΠΕΝΕΔ - contract no.03ΕΔ832).

## *References*

1. Fotopoulos V., Skodras A.: Digital image watermarking: An overview, invited paper, EURASIP Newsletter, ISSN 1687-1421, Vol. 14, No. 4, Dec. 2003, pp. 10-19 (2003)

2. Cox J., Miller L.: The First 50 Years of Electronic Watermarking, EURASIP Journal on Apllied Signal Processing, February 2002, pp. 126-132 (2002)
3. Liu J., Zhang X., Sun J., Lagunas M. A.: A Digital Watermarking Scheme Based on ICA Detection, 4th International Symposium on ICA and BSS (ICA2003), Nara, Japan (2003)
4. Yu D., Sattar F., Binkat B.,: Multiresolution fragile watermarking using complex chirp signals for content authentication, Pattern Recognition, Vol. 39, pp. 935-952 (2006)
5. Lee S., Suh Y., Ho Y.: Lossless Data Hiding Based on Histogram Modification of Difference Images, PCM 2004, LNCS 3333, pp. 340-347 (2004)
6. Varsaki E., Fotopoulos V., Skodras A. N.: A reversible data hiding technique embedding in the image histogram, Technical Report No HOU-CS-TR-2006-08-GR, EAP, Patras (2006)
7. Xiaoping L., Xiaoyun W., Jiwu H.: Reversible Data Hiding Based on Histogram Modification of Wavelet Coefficients, CIS 2005, part II, LNAI 3802, pp. 573-580 (2005)
8. Petitcolas F., Anderson R., and Kuhn M.: Attacks on copyright marking systems, in International workshop on information hiding, LNCS 1525 (Springer-Verlag, Berlin, Germany), pp. 218-238 (1998)
9. Pereira S. and Pun T.: Fast robust template matching for affine resistantimage watermarks, in Proc. 3rd Int. Information HidingWorkshop, pp. 207–218, (1999)
10. Csurka G., Deguillaume F., O'Rauanaidh K., and Pun T.: A Bayesian approach to affine transformation resistant image and video watermarking, in Proc. 3rd Int. Information Hiding Workshop, pp. 315–330 (1999)
11. Lin C., Wu M., Bloom J., Cox I., Miller M., Lui Y.: Rotation, Scale, and Translation Resilient Watermarking for Images, IEEE Transactions on Image Processing, Vol 10, No5 (2001)
12. Lee C., Lee H.: Geometric attack resistant watermarking in wavelet transform domain, Optical Society of America, Vol 13, No 4 (2005)
13. Fang Z., Zhao Y. : Image Watermarking Resisting to Geometrical Attacks Based on Histogram , International Conference on Intelligent Information Hiding and Multimedia, *iih-msp*, pp. 79-82 (2006)
14. Dainaka M., Nakayama S., Echizen I., Yoshiura H.: Dual-Plane Watermarking for Color Pictures Immune to Rotation, Scale, Translation, and Random Bending, International Conference on Intelligent Information Hiding and Multimedia, *iih-msp*, pp. 93-96 (2006)
15. Wang D., Lu P.: Geometrically Invariant Watermark Using Fast Correlation Attacks, International Conference on Intelligent Information Hiding and Multimedia, *iih-msp*, pp. 465-468 (2006)
16. Xu Z. , Wang K., Qiao X.: A Novel Watermarking Scheme in Contourlet Domain Based on Independent Component Analysis, International Conference on Intelligent Information Hiding and Multimedia, *iih-msp*, pp. 59-62 (2006)