Digital Watermarking Using Homogeneity in Image

S. K. Mitra[1], M. K. Kundu[2], C. A. Murthy[2], B. B. Bhattacharya[2] and T. Acharya[3]
[1]Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar 382009, Gujarat, India
suman_mitra@da-iict.org
[2]Indian Statistical Institute
203 B. T. Road
Kolkata 700108, India
{malay, murthy, bhargab}@isical.ac.in
[3]Intel Corporation,
5000 West Chandler Boulevard
AZ 85226, USA
tinku.achrya@intel.com

Abstract—A new technique of digital watermarking for gray-level images is reported in this paper. Digital watermarking/hiding has emerged as a new area of research in connection to Intellectual Property (IP) protection of images. The redundancy in image representation can be exploited successfully to hide some characteristic information in images, without noticeable distortion. Hidden information after extraction, can be used to protect copyright. This article deals with a block-based technique for inserting a copyright mark (invisible logo) into a gray-level image. The robustness of the proposed method has been tested against non-destructive attacks like mean and median filtering.

1. INTRODUCTION

The emergence of the Internet as a popular means of communication has introduced new dilemmas regarding intellectual property. The text and images that exist in electronic form may be duplicated and republished without degradation, attribution, and often without detection. It is difficult to detect such offenses. Even if such cases are found, it may be hard to prove ownership. The current popular formats for images do not allow for any type of proprietary protection. Any information contained in the header either could be manipulated without corrupting the image, or may be lost when printed and scanned back into digital form.

One possible solution to this proprietary problem can be achieved with digital image watermarking [1], [2], [3]. Recently, such techniques have received lot of attention in the research and in the industry community [4]. The objective of this work is to develop a new technique of digital watermarking using homogeneity in an image.

The redundancy in image representation can be exploited successfully to hide some characteristic information, e.g., trademarks, signatures, fingerprints, etc., in ordinary gray or coloured images, without degrading the quality of the original image and with no extra memory space. Hidden information is extracted using suitable extraction algorithm. The extracted information can be used to detect copyright violations, if any.

Digital watermarking or copyright marking is a major subdicipline of information hiding. A watermarking system can be either imperceptible (invisible) or visible. Imperceptible watermarking systems may be more robust towards non destructive attacks where as visible watermarking may be fragile. This type of watermarking system is ideal for image authentication applications. Different approaches have been adopted to provide efficient imperceptible watermarking algorithms. Some works are based on properties of the human visual system and taking advantage of the masking. To achieve the desired robustness, there are algorithms based on either spread-spectrum techniques [5] or on some adaptive techniques [6]. Embedding the watermark information in the least-significant bit (LSB) though is very popular, still more recent systems are applying more sophisticated embedding mechanism, including the cryptographic hash function. There are other methods where the authentication marks are embedded in the coefficients of a transformed image, *eg*. the signature is inserted in DCT or wavelet coefficients [7].

In the present article, we have described a new technique for inserting a logo (a small binary image) into a gray-level image which we intend to protect from copyright violation. The logo is inserted within the image in such a way that it is invisible and survives outside attacks. The robustness of this methodology has been tested against non-destructive attacks like mean and median filtering.

2. WATERMARKING

Concealing information in other objects is usually called steganography. The term has a Greek origin and literally means covered writing. Digital watermarking comes under the umbrella of steganography. In particular, there are two types of watermarking schemes available in the literature [8]. One is visible watermarking and other is imperceptible or invisible watermarking. Here, the second type of scheme is developed. To develop effective methodology for imperceptible

This work is funded by a grant from Intel Corp., USA (PO # CAC042717000), US patent pending-2000

tible digital image watermarking the following points need to be considered.

- Image degradation due to watermarking;
- Robustness against non-destructive attacks;
- Ease of implementation;
- Ratio of information contained in the watermark (logo) to that in the image.

We describe our algorithm for hiding a (16 x 16) binary image (logo), into a (256 x 256), 8 bits/pixel gray-level image. Note that the same methodology can also be used while hiding a larger logo into an image of size more than (256 x 256).

Insertion

First, partition the given (256 x 256), 8 bits/pixel image into non-overlapping square blocks of size (6 x 6). Next, find variances of all blocks. Arrange the blocks in ascending or descending order depending on their variance values. The blocks having small variance values are called *homogeneous* blocks. The homogeneity regions (blocks) of an image is selected using the variance values. However, one can think of other measures too, for the same purpose.

A block is denoted by the location of its starting pixel (i, j). Select only those many blocks (starting from the first block in ascending order), which are needed for hiding the logo image. Only two bits of the logo image will be stored in each block, and hence, 128 blocks are required. The blocks are selected such that the mean gray level values of the blocks are either less than T_1 or greater than T_2, where T_1 and T_2 are certain pre-specified threshold values. The value of T_1 should preferably be close to '0' (minimum possible gray level value), and T_2 should be close to '255' (maximum possible gray level value). However, the 'closeness' of T_1 and T_2 to '0' and '255' respectively, is a relative term, and is strongly image dependent. Users may choose the values of T_1 and T_2 by checking the degradation in the image quality effected by the insertion of the logo.

Arrange the selected blocks in ascending order depending on their location. Note that an (i, j)-th block is less than the (k, l)-th block if

(a) $i < k$, or
(b) $j < l$, if $i = k$.

The mean value of each block truncated to the nearest integer is found. The two least significant bit positions in its 8-bit representation are replaced by two bits chosen from the logo image. Then, each pixel value of each of the selected blocks is replaced by the corresponding changed mean value, making each block to possess zero variance. The (16 x 16) logo image can be thought of as a binary string of length 256; thus first 2 bits of the string is used to modify the mean of the first selected block. The next two bits are used to modify the next homogeneous block and so on. This procedure may lead to a little blocking artifacts in the watermarked image; however, as the block size is very small compared to that of the image, the distortion is often imperceptible. One can expect less distortion due to blocking, if the mother image in which the logo is to be hidden, is of larger size.

The homogeneous blocks which are not needed for hiding, may have variances too close to those of the selected blocks. To ensure robustness, variances of such blocks are increased by an adaptive enhancement procedure described below:

For each such block, let

(i) mean	=	bl_mean (say)
(ii) minimum gray level value	=	bl_min (say)
(iii) maximum gray level value	=	bl_max (say)

Find

(i) $bl\_max - bl\_mean$	=	m (say)
(ii) $bl\_mean - bl\_min$	=	n (say)
(iii) new_max	=	$bl\_max + n$
(iv) new_min	=	$bl\_min - m$

Replace each pixel value (gray_value) of the block by

$$\left[\frac{(new\_max - new\_min)}{(bl\_max - bl\_min)}\right](gray\_value - bl\_min) + new\_min.$$

In this procedure, the mean of each block will remain unchanged, whereas the variance of each block is increased resulting graceful degradation of the image.

The extraction of the logo can be performed as follows.

Extraction

As before, partition the watermarked image (256 x 256), 8 bits/pixel, into non-overlapping square blocks of size (6 x 6). Now, arrange the blocks in ascending/descending order of variances. Blocks having small variance value are identified as homogeneous.

A block is denoted by the location of its starting pixel (i, j). To extract the hidden information, one needs to correctly identify those blocks where the information is hidden. From insertion procedure, it is clear that information is hidden in homogeneous blocks, *i.e.*, whose variance values are small. However, due to non-destructive attacks (mean or median filtering), the variability of those blocks may change to some extent. Further, it is hard to estimate the change in their variance values. Thus, sorting of blocks with respect to their variance values is needed followed by the choice of 128 blocks among them. If the variance values of a block where information is hidden, is changed significantly, one may not be able to extract completely the hidden information.

Using the above order, for each block compute the variance of four pixels which are at the middle of the block. For example, in a (6 x 6) block, consider pixel values which are at (3,3), (3,4), (4,3) and (4,4) positions. It is expected that the pixel values of these four positions will be least affected by non-destructive attacks (mean and median filter). Select those blocks for which the newly computed variance values are close to zero. Note that, one needs to select those many blocks in which the information is hidden. For each of these selected blocks, locate a pixel lying at the middle of the block. For example, in a (6 x 6) block, consider any one of the pixel values which are either at (3,3), (3,4), (4,3), or (4,4) position. The two least significant bits of the selected pixel value provide the information hidden in the block The location of the block gives the position of this 2 bits in the logo image.

The next Section provides the results of the proposed methodology implemented on a 256 $\times$ 256, 8-bit/pixel image. Note that, though the algorithm has been tested on several real life images yet the results of only one image is presented here.

3. RESULTS

The algorithm is coded in Matlab and run on a Sun Ultra-60 workstation. The (16 x 16) binary image (logo) to be hidden is shown in Figure 3. The mother image is (256 x 256), 8 bits/pixel Cathedral (Figure 1). The watermarked image after inserting the logo is shown in Figure 2. Figure 6 depicts the low-variance blocks of the mother image where information is hidden. Figures 4 and 5 show the watermarked image after filtering, from which the logo can be extracted. Zoomed versions of the original image and the watermarked image are shown in Figure 7 and Figure 8 respectively. The value of PSNR regarding image degradation due to watermarking in the proposed method is given in Table 1.

Figure 1. Original "Cathedral" image (256 $\times$ 256, 8bpp) on which the present watermarking scheme is implemented.

The presented watermarking scheme has also been tested with other images. Figures 9, and 10 are two such images, *viz*., "Seafish" and "Zebra" respectively. The corresponding watermarked images of Seafish and Zebra are shown in Fig-

Figure 2. Watermarked "Cathedral" image (Logo inserted)

Figure 3. "Logo" image (16 $\times$ 16, binary) to be inserted.

Figure 4. Corrupted watermarked "Cathedral" image (by mean filter used two times).

Figure 5. Corrupted watermarked "Cathedral" image (by median filter used three times)

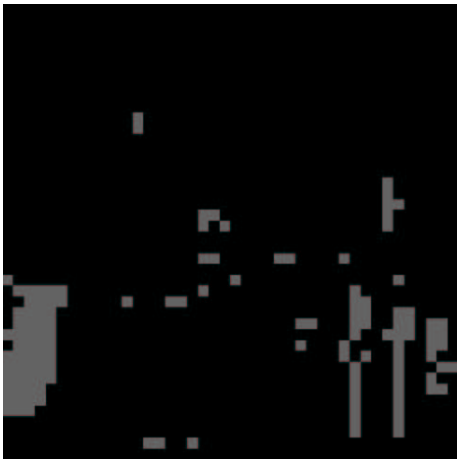

Figure 6. Blocks of the original "Cathedral" image where information (pixel values of binary Logo) is to be hidden.

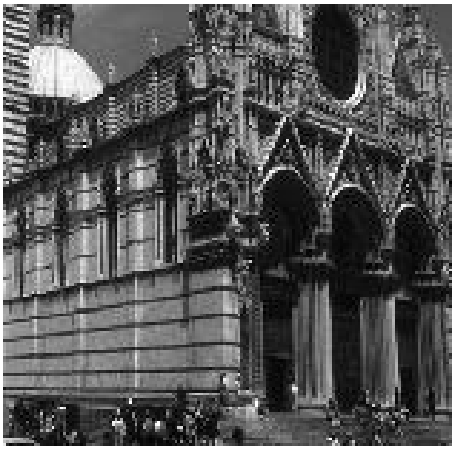

Figure 7. Magnified view of the important portion (where information regarding pixels values of binary Logo is to be inserted) of the original "Cathedral" image.

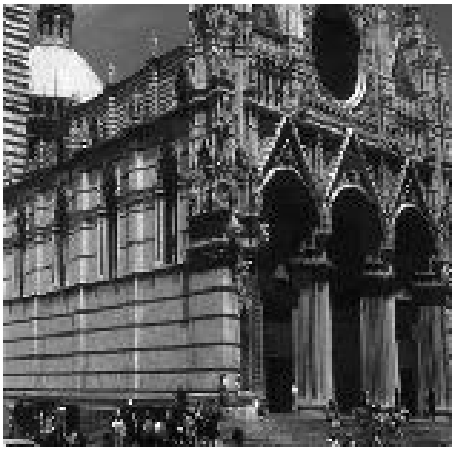

Figure 8. Magnified view of the important portion (where information regarding pixel values of binary logo is inserted) of the watermarked "Cathedral" image

Table 1. Test results showing peak-signal-to-noise ratios of the watermarked image 1, and it's several versions under attacks (use of filters). The status of the Logo retrieved is also provided.

Corruption	PSNR	Retrieval of Logo
Nil	40.17	Yes
Mean Filter (used once)	20.35	Yes
Mean Filter (used twice)	20.17	Yes
Mean Filter (used thrice)	19.65	No
Median Filter (used once)	20.13	Yes
Median Filter (used twice)	20.08	Yes
Median Filter (used thrice)	19.86	yes
Median Filter (used 4 times)	19.68	No

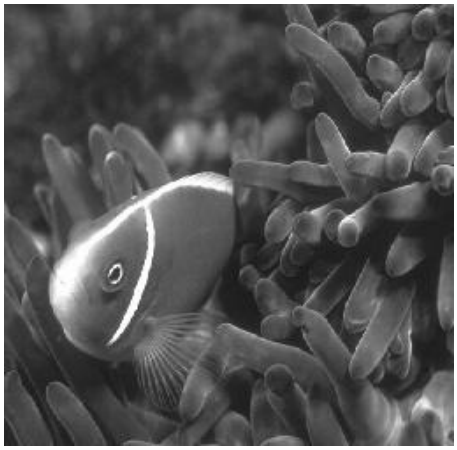

Figure 9. Original "Seafish" image (256 $\times$ 256, 8bpp).

ures 11, and 12 respectively. Table 2 is presenting the experimental results regarding the retrieval status of the Logo when watermarked images are treated with mean and median filters as mentioned earlier. Peak-Signal-to-noise ratio for each case has also been reported.

4. CONCLUSIONS

The present watermarking algorithm is very easy to implement. It provides successful retrieval of the logo not only from the watermarked image but also from the corrupted watermarked image. It has been observed that recovery of the logo is possible even if the watermarked image is corrupted by a mean filter or by a median filter used more than once. The zoomed watermarked image is found to be visually indistinguishable from the original one. The blocking effect is

Table 2. Test results showing peak-signal-to-noise ratio and retrieval status when present watermarking scheme is implemented on "Seafish" and "Zebra" images.

Corruption	Images used			
	Zebra		Seafish	
	PSNR	Retrieval of Logo	PSNR	Retrieval of Logo
Nil	47.28	Yes	41.98	Yes
Mean Filter (used once)	21.29	Yes	30.26	Yes
Mean Filter (used twice)	21.04	Yes	28.98	No
Mean Filter (used thrice)	20.49	No	27.89	No
Median Filter (used once)	21.35	Yes	32.34	Yes
Median Filter (used twice)	21.17	Yes	31.34	Yes
Median Filter (used thrice)	20.87	Yes	30.61	Yes
Median Filter (used 4 times)	20.66	No	30.14	Yes

Figure 10. Original "Zebra" image (256 × 256, 8bpp).

Figure 11. Watermarked "Seafish" image(Logo inserted).

Figure 12. Watermarked "Zebra" image (Logo inserted).

negligible. The robustness of the methodology is being investigated in the case of other non-destructive attacks such as flip, slight rotation, noise and JPEG compression. The quality of the watermarked image in this method, will depend on the relative information content the mother image and the logo.

REFERENCES

[1] R. Anderson, *Information Hiding, Proceedings of the 1st Workshop on Information Hiding, LNCS-1174*, Springer Verlag, New York, 1996.

[2] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, pp. 26–34, 1998.

[3] S. Katzenbesser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House, USA, 1999.

[4] I. J. Cox and M. L. Miller, "A review of watermarking and importance of perceptual modeling," in *SPIE Proceedings on Human Vision and Electronic Imaging, II, Vol. 3016*, 1997.

[5] I. Cox, J. Kilian, and T. Leighton, "Source spread spectrum watermarking for multimedia," *IEEE Transaction on Image Processing*, vol. 6, pp. 1673–1687, 1997.

[6] C. I. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 16, pp. 525–539, 1998.

[7] Y. S. Kim, O. H. Kwon, and R. H. Park, "Wavelet based watermarking method for digital images using the human visual system," *Electron. Lett. IEE*, vol. 35, no. 6, pp. 466–468, 1999.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding - A Survey," in *Proceedings of the IEEE, Vol. 87*, 1999, pp. 1062–1078.