Journal of Computer Science 2 (1): 114-117, 2006
ISSN 1549-3636

An Optimization Approach for Selecting Blocks of Embedding Process in Robust Watermarking System

[1]Ababneh M.F. Mohammad, [2]Naseem Masoud Asad
[1]Balqa' Applied university, Salt, Jordan, [2]Ministry of education, Jordan

Abstract: This study, discusses several kinds of attacks that may meet the watermarked image such as JPEG compression, Gaussian noise and median filter. The study introduces an approach capable of selecting the optimal blocks in cover image to be used in embedding process. Also, in this study, we propose a technique in robust digital watermarking system looking for finding a relation between the contrast of cover image and robustness to increase the resistance of previous attacks.

Key words: Watermarking, information hiding, security, robustness, contrast

INTRODUCTION

Information hiding is a general term that can be implemented using several techniques. The main goal is how we can conceal data inside media such as texts, images, audio and video[1].

There are various uses of information hiding, but all of these uses are related to insurance of security especially in military filed and e-commerce. Information hiding techniques should insure that concealed data would be invisible to the naked eye[2].

Nowadays, two sciences of data hiding have been emerged, steganography and watermarking. Steganography is about concealing the very existence of hidden data in innocent computer files such as digital pictures or digital audio[3]. It comes from Greek steganos, which means (covered or secret) and graphy which means (writing or drawing), literally means "covered writing". Watermarking is about hiding imperceptible and irremovable data in a cover media for intellectual property protection purposes; thus, it extends some information that may be considered attributes of the cover, such as copyright[4].

Digital watermarking describes methods and technologies that allow to hide information, for example a number or text, in digital media, such as images, video and audio[5]. The embedding takes place by manipulating the content of the digital data, that means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark has to be robust or fragile, depending on the application. With robustness, we refer to the capability of the watermark to resist to manipulations of the media, such as lossy compression, scaling and cropping, just to enumerate some. Fragility means that the watermark should not resist tampering, or only up to a certain extent[6].

Digital watermarks have several desirable characteristics. The watermark should be integrated with the image content so it cannot be removed easily without severely degrading the image. The watermark should be fairly tamper resistant and robust to common signal distortions, compression and malicious attempts to remove the watermark. The watermark can be made invisible to the human eye, but still readable by computer[7].

An adaptive digital image watermarking technique for copyright protection (ADIW): To meet both invisible and robust requirements, we will adaptively modify the intensities of some selected pixels as large as possible and this modification is not noticeable to human eyes. In addition, to prevent tampering or unauthorized access, the watermark is first permutated into scrambled data. The block diagram of watermarking system is depicted in Fig. 1.

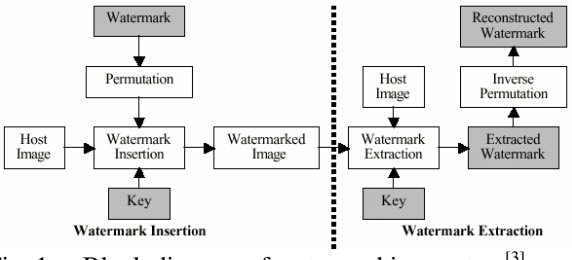


Fig. 1: Block diagram of watermarking system[3]

Watermark embedding process: The embedded watermark must be invisible to human eyes and robust to most images processing operations. To meet these requirements, a bit of binary pixel value (0 or 1) is

Corresponding Author: Ababneh M.F. , Balqa' applied University, Salt, Jordan.

embedded in a block of the host image. Before insertion, the host image is decomposed into N*N blocks. Depending on the contrast of a block, pixels in the block are adaptively modified to maximize robustness and guarantee invisibility. The position or block for embedding is selected by a pseudo-random number generator using a seed value k[8].

Let **B** be the selected block and g_{max}, g_{min} and g_{mean} represent the maximal, minimal and average intensities of the block, respectively. That is,

$$g_{max} = \max(b_{ij}, 0 \le i, j < N),$$
$$g_{min} = \min(b_{ij}, 0 \le i, j < N), \text{ and}$$
$$g_{mean} = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} b_{ij},$$

Where, b_{ij} represents the intensity of the $(i, j)^{th}$ pixel in block B. Assume that the embedded pixel value b_w is 0 or 1. The embedding process modifies the intensities of pixels in the block **B** according to the following rules[8]:

$$\begin{aligned}
&(1)\ b_w = 1: \\
&\quad g' = g_{max} \quad \text{if } g > g_{mean}, \\
&\quad g' = g+\delta \quad \text{if } g \le g_{mean}, \\
&(2)\ b_w = 0: \\
&\quad g' = g_{min} \quad \text{if } g < g_{mean}, \\
&\quad g' = g-\delta \quad \text{if } g \ge g_{mean},
\end{aligned}$$

Where, **g'** is the modified intensity and δ is a small value used to tune the intensities. The embedding of the watermark depends on the content of each block. If the block is of higher contrast, the intensities of pixels will be modified greatly. Otherwise, the intensities are tuned slightly. Thus, the proposed algorithm can adaptively modify the content of a block. Let blocks **B** and **B'** denote the original and watermarked blocks, respectively. The sum of pixel intensities of **B'** will be larger than that of **B** if the inserted watermark pixel value $\mathbf{b_w}$ is 1. On the contrary, if the inserted watermark pixel value $\mathbf{b_w}$ is 0, the sum of pixel intensities of **B'** will be smaller than that of **B**[8].

Watermark extraction: The extraction of a watermark is similar to the embedding process while in a reverse order. The extraction of a watermark must make reference to the original host image. First, using the seed value, k, to generate a sequence of positions or blocks where the watermark is embedded. For each selected position, let **B** and **B'** represent the corresponding blocks of the original host image and watermarked image, respectively. Compute the sum of pixel intensities, $\mathbf{S_o}$ and $\mathbf{S_w}$, of **B** and **B'**. The retrieved watermark bit value $\mathbf{b_w}$ is determined by the following:

$$\begin{aligned}
b_w &= 1 \quad \text{if } S_w > S_o, \\
b_w &= 0 \quad \text{if } S_w \le S_o.
\end{aligned}$$

The extracted watermark bit values**,** $\mathbf{b_w}$**'s**, are then inversely permutated to get the reconstructed watermark[8].

Proposed technique: The proposed technique presented here, can be enrolled into the blind category. This technique is characterized by the spatial domain of it is processing domain, the invisibility of its modification type, the modification type is additive, the availability of the original data is blind, the cover image used is gray, the water type is a binary image (0,1) and finally this proposed technique has a symmetric (public) privacy.

Embedding process: The input of embedding process consists of watermark (or encrypted watermark), cover media and key and the output will be the watermarked media. The main differences between all various embedding techniques are in encryption process and the key of embedding process. Here, we develop the Adaptive Digital Image Watermarking technique (ADIW) described earlier.

The proposed technique uses the same embedding equations that are used in ADIW technique, the difference between the proposed technique and ADIW technique is in the cover image block selection. While the ADIW adopts the random selection algorithm, we have develop an algorithm that looks for the optimal cover image block which results in a better extracted watermark.

Definition of the optimal cover image block depends on the contrast of block that used to hide watermark has the main reason to choose it as a measurement of selection blocks process. Some kinds of attacks decrease the intensities of pixels such as JPEG compression and Gaussian noise, while another kinds of attacks increase the intensities of pixels such as median filter. So that, using high contrast block to embed watermark pixel value will resist some kind of attacks such as JPEG compression. On the other hand, using low contrast block to embed watermark pixel value will resist some kind of attacks such as median filter.

Using high contrast blocks: If the block is of higher contrast, the intensities of pixels will be modified greatly and the difference between S_W (summation of block intensities in watermarked image) and S_O (summation of block intensities in cover image) will be large. So that, this large of difference may able to prevent breaking the origin relation between S_W and S_O if the watermarked image attacked by JPEG compression and Gaussian noise, since, these kind of attacks will decrease the intensities of block pixels and this modification may break the origin relation between S_W and S_O. On the other hand, if the block is of lower contrast, the intensities of pixels are tuned slightly and the difference between S_W and S_O will be small. So that,

this small amount of difference may not be able to prevent breaking the origin relation between S_W and S_O if the watermarked image attacked. For example, let us assume that the embedded pixel value **P** is 1, $\mathbf{B_O}$ be the origin block and $\mathbf{S_O}$ is the summation of intensities in $\mathbf{B_O}$, $\mathbf{B_W}$ be the watermarked block and $\mathbf{S_W}$ is the summation of intensities in $\mathbf{B_W}$, as shown in Fig. 2. From Fig. 2a, we can observe that S_O=185, S_W=225 with difference = 40. This means that $S_W > S_O$, which is an essential required for hiding binary 1.

10	15	30
35	30	20
15	20	10

(a)

15	20	35
35	35	25
20	25	15

(b)

Fig. 2: (a) B_O with low contrast (b) The watermarked block B_W

Now, if an attack modifies the intensities of B_W such that to make the value of S_W=175 (i.e. Decreasing value=50), this makes $S_W < S_O$, which indicates that the embedded pixel was binary 0, giving a wrong result to the original embedded pixel. It is clear now that if B_O has low contrast, then it will be more sensitive for this kind of attacks modification and will give us wrong result. But on the other hand, if B_O has high contrast then, it will be less sensitive of attack modification and will give us right result as explained below:

10	20	30
40	50	60
70	80	90

(a)

15	25	35
45	90	90
90	90	90

(b)

Fig. 3: (a) BO with high contrast (b) The watermarked block BW

Depending on Fig. 3, S_O=450, S_W=570 and the difference = 120, the relation between S_O and S_W is $S_W > S_O$. This relation indicates that B_W represents embedded pixel with value 1, but if modification of attack decrease the intensities of B_W such that S_W=520 (i.e. Decreasing value=50), the relation will not be changed to $S_W < S_O$. Note that, when the block used for embedding pixel with value=0, the modification of attack will not effect on the result.

Using low contrast blocks: In some cases, it is better to select the low contrast block to be used for embedding process, choosing high or low contrast block depends on attack behavior. Median filter may increases or decreases the intensity of pixel value, since it depends on the intensity of the neighborhood around each pixel in the image. Assume that the neighborhood of pixel is in high contrast, then the probability of high modification (either increasing or decreasing) will be large enough to break the relation between S_O and S_W. On the other hand, if the neighborhood of pixel is in low contrast, then the probability of high modification (either increasing or decreasing) will be small enough to keep the relation between S_O and S_W.

The Proposed technique looking for high contrast and low contrast blocks in origin image to hide two copies of watermark, one of them embedding in most high contrast blocks (to resist such as JPEG compression and Gaussian noise attacks) and the other one embedding in most low contrast blocks (to resist such as median filter). Almost, contrast of block depends on the difference between max and min intensities of block to indicate, if it is either low or high contrast. If the difference is large, then block has high contrast otherwise it has low contrast.

Watermark extracting: The extraction of a watermark is similar to the embedding process in ADIW but in reverse order. But there is main difference which is that in extracting process of ADIW must use the origin cover image (non-blind) while the proposed technique use sorted array without using cover image (blind) through extracting process. An extracted watermark must be decrypted in reverse order of encryption process.

RESULTS

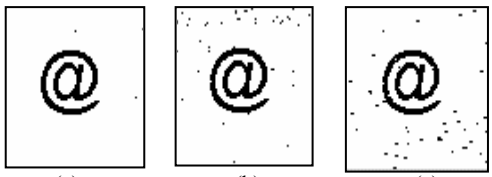
In order to exploit our technique, we have exposed the water marked image produced by the method to the most likely to happen noise attacks; Gaussian noise, JPEG compression and median filter. We then extracted the watermark by the three methods discussed earlier.

Figure 4, shows the effect of adding Gaussian noise on the watermarked image and Fig. 5 shows the effect on the extracted watermark using three different methods. Figure 6 shows the effect of JPEG Compression on the extracted water mark using three different approaches. Finally Fig. 7 shows the effect of Median filter on the extracted watermark using the same three approaches.

Fig. 4: Watermarked image after adding Gaussian noise

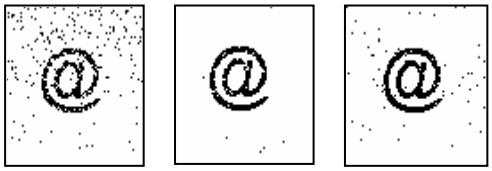
(a) (b) (c)

Fig. 5: (a) Extracted watermark using high contrast blocks. (b) Extracted watermark using low contrast blocks. (c) Extracted watermark using ADIW technique



(a) (b) (c)

Fig. 6: (a) Extracted watermark using high contrast blocks. (b) Extracted watermark using low contrast blocks. (c) Extracted watermark using ADIW technique



(a) (b) (c)

Fig. 7: (a) Extracted watermark using high contrast blocks. (b) Extracted watermark using low contrast blocks. (c) Extracted watermark using ADIW technique

Analysis: From the above results, we can see that Gaussian noise causes a large decrease to the pixels intensities. So, it is better to use high contrast blocks in cover image to hide watermark because they have more resistance than low contrast block and ADIW selected blocks.

JPEG compression has a similar effective behavior like Gaussian noise, it means that both of them make decrements modification on the pixel intensities. But the main deference is, JPEG tunes slightly the intensities of pixels value, so that the effective will not be sensitive for naked eye. It is clear now that, using high contrast blocks to embedding the watermark is better than using low contrast blocks when watermarked image exposed to JPEG compression.

In some cases it is better to select the low contrast block to be used for embedding process, choosing high or low contrast block depends on attack behavior. Median filter may increase or decrease the intensity of pixel value, since it depends on the intensity of the neighborhood around of each pixel in the image. Assume that the neighborhood of pixel is in high contrast, then the probability of high modification (either increasing or decreasing) will be large enough to break the relation between SO and SW. On the other hand, if the neighborhood of pixel is in low contrast, then the probability of high modification (either increasing or decreasing) will be small enough to keep the relation between SO and SW. So, using low contrast blocks to embedding the watermark is better than using high contrast blocks when watermarked image exposed to median filter.

CONCLUSION

In this study, we have proposed an adaptive image watermarking algorithm. The watermark adopted is a visually meaningful binary image such that human eyes can easily judge the extraction result. To embed a watermark in the host image, the proposed approach utilizes the sensitivity of human visual system to adaptively modify the contents of a block. The main goal is to select the optimal blocks of cover image to be used for hiding the watermark pixels. Selection of the optimal blocks depend on the contrast of cover image blocks, this optimization process gives better results than the selection process that is used in ADIW technique.

Experimental results show that the proposed algorithm is robust to common image operations such as median filter, JPEG image compression and Gaussian noise. In some cases, selecting a high contrast block gives better results than selecting a low contrast block, it depends on attacks behavior.

REFERENCES

1. Petitcolas, F., R. Anderson and M. kuhn, 1999. Information hiding-A survey. Proc. IEEE., 87: 1062-78.
2. Craver, S., N. Memon, B.L. Yeo and M.M. Yeung, 2002. Can invisible watermarks solve rightful ownerships? IBM Technical Report RC 20509, IBM Research, IBM Cyber J., http://www.research.ibm.
3. Chang-Hsing Lee, 1995. National Science Council of R.O.C. under Contract. NSC87-2218-E-034-001.
4. Khan David, 1996. The History of Steganography. Information Hiding: First Intl. Workshop Proc., Lecture Notes in Computer Science, Springer, 1174: 1-5.
5. Davern, P. and M. Scott, 2000. Steganography its history and its application to computer based data files, computer application. Ca-0759, Dublin City University, Ireland.
6. Johnson, N.F., 1999. Steganography: An internet survey. http://ise.gma.edu/~csis.
7. Jiri Fridrich and M. Goljan, 1999. Comparing Robustness of Watermarking Techniques. SPIE Security and Watermarking of Multimedia Content. San Jose, C.A.
8. Cox, I., M. Miller and J. Bloom, 2001. Digital Watermarking. Morgan Kaufmann Publishers.