http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (2): 246-256, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.246.256

Effective Hill Climbing Algorithm for Optimality of Robust Watermarking in Digital Images

[1]C.H. Wu, [1,2]Yen Zheng, [1]W.H. Ip, [3]Zhe-Ming Lu, [1]C.Y. Chan and [1]K.L. Yung
[1]Department of ISE, The Hong Kong Polytechnic University, Hunghom, Hong Kong, China
[2]School of Information Science and Technology, Sun Yat-Sen University, Guangdong, China
[3]The Institute of Astronautic Electronic Engineering,
School of Aeronautics and Astronautics, Zhejiang University, China

Abstract: Due to the explosion of data sharing on the internet and the massive use of digital media, especially digital images, there is great interest by image owners in copyright protection. The genetic watermarking methods were previously shown to optimize the conflicting requirements of robustness and invisibility. However, the genetic watermarking methods have limitation in considering perceptually significant or non-significant regions in the selection process, so they do not always offer better imperceptibility. In addition, the computational resource required by Genetic Algorithm (GA) is high when comparing it to other heuristic methods. Thus, the current study is focused on an optimization-based Dither Modulation watermarking scheme for digital images in a more efficient and effective manner. The watermark imperceptibility and robustness are taken into consideration at the same time. A hill climbing algorithm, which has a simple computational process, is employed for optimizing these two conflicting requirements. Since, Peak Signal-to-Noise Ratio (PSNR) may not be an effective imperceptibility measure presented previous genetic watermarking methods, Watson's perceptual model is employed to quantify the watermarked image distortion as it is consistent with Human Visual System (HVS). Several commonly used watermarking attacks are considered in the optimization process. Experimental results demonstrated that the proposed algorithm is robust and more time efficient than the previous GA based methods.

Key words: Robust watermarking, dither modulation, watson's perceptual model, hill climbing optimization, genetic algorithm

INTRODUCTION

One of the applications of digital watermarking is to embed a watermark signal into the host data for the purpose of copyright protection (Chang *et al*., 2002). Research on copyright protection of images is still at a blooming stage; however, no reported method is totally immune against all malicious attacks, effectively. It is obvious that the watermark should be robust and imperceptible for copyright protection but the requirements of imperceptibility and robustness conflict with each other.

Recently, two kinds of methods have emerged to strive for a balance between the robustness and imperceptibility. The first one is to make use of Human Visual System (HVS) based algorithms. For examples, Podilchuk and Zeng (1998) proposed a JND based watermarking algorithm in the Discrete Cosine Transform (DCT) domain and the Discrete Wavelet Transform (DWT) domain separately. A spatial method was devised by Qi *et al*. (2008), which embeds watermarks adaptively based on the luminance masking, texture masking and the edge masking. The second one applies intelligent optimization algorithms, such as Genetic Algorithms (GA), to watermarking. The basic idea of the evolutionary optimization based methods is to maximise a fitness function which takes the robustness and the imperceptibility into account simultaneously. GA can be used for optimizing the fundamentally conflicting requirements of imperceptibility, robustness and capacity. It is a fact that GA has been widely used in optimizing watermarking problems. Kumsawat *et al*. (2005) devised spread spectrum watermarking in the discrete multi-wavelet domain by applying GA. Shieh *et al*. (2004) proposed a GA based robust watermarking algorithm in the DCT domain. Wei *et al*. (2006) improved the speed of the genetic watermarking algorithm proposed by Shieh *et al*. (2004) and enhanced both the robustness and imperceptibility by adopting a new embedding and extracting method, in 2006. Recently, Huang *et al*. (2009) further improved the watermarking framework of Shieh *et al*. (2004) by taking the capacity into account.

Corresponding Author: C.H. Wu, Department of ISE, The Hong Kong Polytechnic University, Hunghom, Hong Kong, China

However, Maity and Kundu (2009) have pointed out two main limitations of the existing GA based methods. Firstly, GA does not consider perceptually significant or non-significant regions in the selection process and knowledge of the cover image characteristics, so it does not always offer better imperceptibility. Secondly, the Peak Signal-to-Noise Ratio (PSNR) may not be an effective imperceptibility measure presented in the objective function.

In the research, the focus is on robust and efficient watermarking based on the optimization approach. Thus, an optimized image watermarking algorithm in the DCT domain is proposed. The proposed method adopts the Watson's model as the image quality measurement, as it is consistent with HVS.

OVERVIEW OF THE WATERMARKING ALGORITHM

Here, there is a review of the related techniques of watermarking applied in the proposed algorithm. The proposed algorithm embeds an invisible watermark by modifying some DCT coefficients through dither modulation.

An invisible watermark should be resistant to different kinds of destruction, namely attacks, while the distortions introduced by the watermarking process must be low, such that the quality of the image is preserved. Thus, it should be useful in verifying the copyright ownership of an image suspected of misappropriation or copyright infringement. Embedding a watermark in low frequency bands leads to high robustness but low imperceptions, while low robustness and high imperceptions can be achieved by embedding a watermark in high frequency coefficients. Therefore, a key aspect of a watermarking algorithm is the balance between watermark robustness and visual imperceptions. The performance of a watermarking algorithm can be evaluated by the equation below.

$$\text{Score} = \text{Imgquality} + \lambda \cdot \text{Wquality} \quad (1)$$

Imgquality denotes the measurement of the quality of the watermarked image. Different measurements can be employed, for example, the PSNR and the image quality index (Wang and Bovik, 2002). HVS based models, such as the Watson's perceptual model (Watson, 1993), are more complicated but are drawing increasing attention from researchers. In this study, Watson's model is used for the image quality measurement. Wquality denotes the quality of the recovered watermark after attack. It demonstrates the robustness of the watermarking algorithm. The commonly used measurements are the Normalized Cross-correlation (NC) and Hamming Distance (HD) between the original watermark and the extracted watermark. As the embedded watermark is binary, the HD is adopted. λ controls the balance between the conflicting requirements of watermark robustness and visual imperceptions. A large λ means more attention is paid on the robustness and a small λ means the watermarked image quality is more important. Higher scores of Eq. 1 mean better performance of the watermarking algorithm. Therefore, the watermarking algorithm should be designed to find the optimal embedding locations in order to maximize the performance scores. In the proposed algorithm, it is formulated as an optimization problem and hence a hill climbing optimization algorithm is proposed, which is more efficient, effective and simpler than the previous GA based approaches applied to watermarking problems.

Watson's perceptual model: Watson describes a model based on 8×8 DCT transform to estimate the perceptual difference between images (Watson, 1993). Watson's model consists of a sensitivity table, a luminance masking effect and a contrast masking effect.

The entry t(i, j) of the sensitivity table denotes the minimal amount of change that produces a Just Noticeable Difference (JND) at the position (i, j) in a 8×8 DCT block. The table under some chosen parameters can be found by Cox *et al.* (2007) work. The role of luminance masking is to compensate the sensitivity table under different average intensities (DC coefficient) for a specific 8×8 DCT block.

$$t_L[i,j,k] = t[i,j](C_0[0,0,k]/C_{0,0})^{a_T} \quad (2)$$

It is clear from Eq. 2 that $t_L(i, j, k)$ denotes the compensated sensitivity table for the (i, j) entry in the kth block. $C_0(0, 0, k)$ is the DC coefficient of the kth block and $C_{0,0}$ is the average of all DC coefficients in the whole image. a_T is set to a constant value of 0.649 according to Watson (1993) work.

The role of contrast masking is to further compensate the sensitivity table as the energy present at a particular frequency, which will reduce the visibility of a change in the frequency.

$$t_{LC}[i,j,k] = \max\{t_L[i,j,k], C_0[i,j,k]^{w[i,j]} \bullet t_L[i,j,k]^{1-w[i,j]}\} \quad (3)$$

It is clear from Eq. 3 that $t_L(i, j, k)$ denotes the compensated sensitivity table by contrast masking and w(i, j) is a constant between 0 and 1. According to Watson (1993), it is suggested that w(i, j) should be set to 0.7 for all i and j.

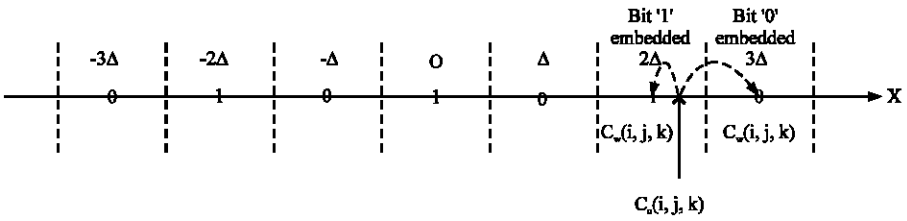

Fig. 1: Illustration of dither modulation

Finally, the perceptual distortions between the watermarked image and the original image are obtained through the following equation:

$$D_{watson} = \left(\sum_{i,j,k} \left| \frac{C_w[i,j,k] - C_o[i,j,k]}{t_{LC}[i,j,k]} \right|^p \right)^{1/p} \quad (4)$$

where, $C_w(i, j, k)$ and $C_o(i, j, k)$ denote the DCT coefficients of the watermarked image and the original image and p is recommended as 4.

Dither modulation: The Quantization Index Modulation (QIM) watermarking embedding algorithm was first proposed by Chen and Wornell (2001). The QIM system has considerable performance advantages over previously proposed spread-spectrum systems. The basic idea of QIM is to quantize the host data to different quantization intervals according to the watermark bit. Dither modulation is a most popular realization for QIM.

As a simple example shown in Fig. 1, a scalar uniform quantizer is set with step size Δ. X is a real axis equally divided by Δ. Each interval is mark by 1 or 0. $C_o(i, j, k)$ is the DCT coefficient in which a watermark bit is to be embedded. According to the watermark bit to be embedded, $C_o(i, j, k)$ is dithered to the center of its nearest interval 1 or 0. $C_w(i, j, k)$ is the watermarked and dithered version of $C_o(i, j, k)$. If $C_w(i, j, k)$ lies in interval 1, the watermark bit is embedded as 1, otherwise the watermark bit 0 is embedded. Therefore, the maximum modification for a coefficient is Δ and it controls the performance of the algorithm, where a larger Δ means more robustness but more image distortion introduced.

PROPOSED WATERMARKING ALGORITHM

The input image X_o is of size M×N. The goal is to embed a robust binary watermark W into the DCT coefficients of X_o. The watermarked image is denoted by X_w. In this study, a 4×4 block DCT is performed on the image X_o and $C_{4o}(i, j, k)$ denotes the original DCT coefficients in row i and column j of the kth 4×4 block. $C_{4w}(i, j, k)$ is the watermarked version. Each DCT block is embedded with one watermark bit. Therefore, the size of the watermark is M/4×N/4. The key issue of the algorithm is how to select a DCT AC coefficient in order to embed a watermark bit in a 4×4 block. In this study, a hill climbing algorithm is employed for the solution.

Watermark embedding and extracting: Before embedding, the binary watermark image W is pseudo-randomly permuted with a predefined key, key, which is generated to increase the robustness.

$$W_p = \text{permute } (W, \text{ key}) \quad (5)$$

where, W is the original watermark and W_p is the permuted watermark.

In the kth block, assume the watermark to be embedded is $W_p(k)$ and the selected DCT coefficient is $C_{4o}(i, j, k)$. The goal is to modify $C_{4o}(i, j, k)$ and then to obtain $C_{4w}(i, j, k)$ based on the dither modulation. According to the sign of $C_{4o}(i, j, k)$ and the watermark bit $W_p(k)$, there are totally four combinations, as shown in Eq. 6 to 9, where m is the integer quotient and r is the remainder of $C_{4o}(i, j, k)$ divided by Δ, shown in Eq. 10 to 11. The quantization step Δ controls the robustness and perceptions of the embedded watermark.

- If $C_{4o}(i, j, k) \geq 0$ and $W_p(k) = 1$

$$C_{4w}[i,j,k] = \begin{cases} 2q\Delta & \text{if } m = 2q \\ 2q\Delta + 2\Delta & \text{if } m = 2q+1 \text{ and } r \geq 0 \\ 2q\Delta & \text{if } m = 2q+1 \text{ and } r < 0 \end{cases} \quad (6)$$

- If $C_{4o}(i, j, k) \geq 0$ and $W_p(k) = 0$

$$C_{4w}[i,j,k] = \begin{cases} 2q\Delta+\Delta & \text{if } m = 2q \text{ and } r \geq 0 \\ 2q\Delta - \Delta & \text{if } m = 2q \text{ and } r < 0 \\ (2q+1)\Delta & \text{if } m = 2q+1 \end{cases} \quad (7)$$

- If $C_{4o}(i, j, k) < 0$ and $W_p(k) = 1$

$$C_{4w}[i,j,k]=\begin{cases}-2q\Delta & \text{if } m=-2q\\ -2q\Delta & \text{if } m=-(2q+1) \text{ and } r\geq 0\\ -2q\Delta-2\Delta & \text{if } m=-(2q+1) \text{ and } r<0\end{cases} \quad (8)$$

- If $C_{4o}(i, j, k)>0$ and $W_p(k) = 0$

$$C_{4w}[i,j,k]=\begin{cases}-2q\Delta+\Delta & \text{if } m=-2q \text{ and } r\geq 0\\ -2q\Delta-\Delta & \text{if } m=-2q \text{ and } r<0\\ -(2q+1)\Delta & \text{if } m=-(2q+1)\end{cases} \quad (9)$$

$$m=\text{floor}\left(\frac{C_{4o}[i,j,k]}{\Delta}+0.5\right) \quad (10)$$

$$r=C_{4o}[i,j,k]-m\Delta \quad (11)$$

where, floor() is the operation of rounding towards negative infinity. Watermark extraction can be easily carried out by checking the parity of m'.

$$m'=\text{floor}\left(\frac{C_{4w}[i,j,k]}{\Delta}+0.5\right) \quad (12)$$

if m' is odd, the extracted watermark bit is 0, otherwise it is 1.

After all watermark bits, W_p', are extracted, the reconstructed watermark, W', is obtained by inverse permuting W_p' under key.

$$W'=\text{inverse permute } (W_p', \text{ key}) \quad (13)$$

Embedding location selection: As mentioned earlier, a set of DCT coefficients should be selected in order to maximize Eq. 1. In this study, a hill climbing optimization algorithm is employed to solve the problem. In order to accelerate the watermarking process, the embedding process is performed independently for each 16×16 block, which is called a macroblock and the watermark bits are embedded macroblock by macroblock. One watermark bit is embedded into each 4×4 block in a macroblock, therefore, a total of 16 bits are embedded into one macroblock. The objective function can be defined as:

$$\text{Score}=-D_{watson}(MB,MB_w)+\sum_{i=1}^{n}\lambda\cdot H_i(W,W') \quad (14)$$

It is clear that $D_{watson}(MB, MB_w)$ denotes Watson's perceptual distortions between the original macroblock and the watermarked macroblock. $H_i(W, W')$ is the Hamming Similarity (HS) between the original watermark bits and the extracted watermark bits for the ith attack. HS is defined as the ratio between the correctly recovered watermark bits and the total watermark bits embedded. λ controls the balance between robustness and imperceptions, given that i = 1,2,...n. To summarize, the whole embedding procedure is iterated below:

- **Step 1:** The host image is segmented into macroblocks and each macroblock is further divided into 16 blocks of size 4×4. A 4×4 DCT transform is performed for these blocks
- **Step 2:** A macroblock, MB, is chosen, for watermark bits embedding. An embedding location for each block in the macroblock is randomly chosen. These locations form a 16 dimension vector, $\vec{L}$
- **Step 3:** The watermark is embedded into the macroblock based on the location vector, $\vec{L}$, according to Eq. 6 to 11. The macroblock is inverse transformed to obtain the watermarked version, MB'. Watson's perceptual distortions between MB and MB' are computed. Then, N kinds of attack are performed on the MB'. The watermark bits for each attacked macroblock are extracted and then the HS values between all extracted watermarks and original watermark for N kinds of attacks are calculated. Finally, a performance score is obtained according to Eq. 14 under the current location vector, $\vec{L}$
- **Step 4:** The location vector is optimized through hill climbing. There are three layers of iterations for the hill climbing. The top layer is the number of hill climbing iterations that the user desires. The second layer is for each dimension stored in $\vec{L}$ and the third layer is the value of $\vec{L}$ (i) which is iterated from the lowest frequency band to the highest band. In each iteration, step 3 is executed. If the newly obtained scores are higher than the previous one, $\vec{L}$ will be replaced by the current embedding locations, otherwise, the current embedding locations will be discarded. Finally, a location vector with the highest score will be obtained and the watermark bits will be embedded into the macroblock, based on this optimal location vector
- **Step 5:** The process proceeds to the next microblcok and executes steps 2 to 4 until all macroblocks are optimized

The concept of the watermarking scheme and the pseudo code of the main watermarking embedding procedure are shown in Fig. 2 and 3.

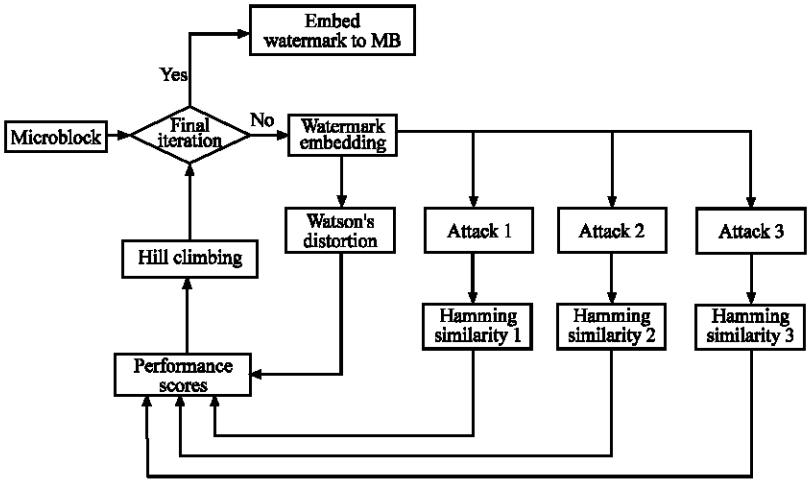

Fig. 2: The illustration of the watermarking embedding scheme

```
For Macroblock=1 to NumofMB

 IterTime=2;                    % Iteration times for Hill Climbing
   OriginalMB=GetMBfromImg (Macroblock) ;
For i=1 to 16                    %watermark bit to be embedded
   MarkBits[i]=WatermarkImg[(NumofMB-1)*16+i];
   End
   For i=1 to 16                    % randomly assigned locations
    L[i]=Ceil(1+15*Rand());
   End
   For i=1 to NumofAttack              % Weighting for each attack
    Attackweighting[i]=24;
   End
   Score=-inf;
   For  HillClimbIter=1 to IterTime
         For  BlockIndex=1 to 16
            For  EmbeddingLocation=2 to 16
               CurrentScore= 0;
               L[BlockIndex]= EmbeddingLocation;
               MarkedMB=EmbedMarkintoMacroblock(L ,OriginalMB);
                        WatsonDistortion=PercuptualDistortion (MarkedMB,OriginalMB);
                     CurrentScore= CurrentScore-WatsonDistortion
               For AttackIndex=1 to NumofAttack
                 PerformAttack(MarkedMB,AttackIndex);
                 ExtractedMark=ExtractWaterMark(MarkedMB);
                 H=CalculateHammingSimilarity(ExtractedMark,OriginalMark)
                          CurrentScore= CurrentScore+AttackWeighting(AttackIndex)*H;
                    End
                  If(CurrentScore> Score)
                     Score= CurrentScore;
                     BestL=L;
       else
                     L=BestL;
        End
                End
  End
End
```

Fig. 3: The pseudo code of the watermarking embedding of macroblocks

EXPERIMENTAL RESULTS AND ANALYSIS

Extensive experiments have been conducted for several well-known test images, including the Airplane (F16), Lena, Pepper, Baboon, Cameraman and Goldhill. The size of the first three images is 512×512 and the last three are of size 256×256. All experiments have been conducted in the Croucher Laboratory of Product

Fig. 4: Test images and the watermark

Mechatronics in The Hong Kong Polytechnic University from July-2009 to April-2010. The logo watermark is more convincing than the binary decision result obtained by using pseudo-random bits as watermark (Shen *et al*., 2005), hence the meaningful binary logo image has been adopted as the watermark. The watermark is the frog image. The size of the watermark for the first three images is 128×128 while the one for the last three images is 64×64. The test images and the watermarks are shown below (Fig. 4).

The aim of the simulations is to verify the proposed robust watermarking method, so inputting attacks is required. However, consideration for the attacked images is also necessary so that they should still maintain meaningfulness and commercial values. Thus, attacks should be properly selected. For example, image cropping is less suitable as an attack because too much information is lost and the subjective image quality is highly degraded. In the simulations here, three kinds of attacks recommended in the previous literature have been chosen (Petitcolas *et al*., 1998; Petitcolas, 2000; Shieh *et al*., 2004), namely, JPEG compression with a quality factor of 75, Low-Pass Filtering (LPF) and Median Filtering (MF), to incorporate into Eq. 14.

In order to see the influence of different weighting (λ) of the watermarked image quality term and robustness term in Eq. 14, λ is set to 12, 16, 20, 24 and 28, respectively for the images. By taking Cameraman as an example, all three attacks have the same λ values with two iterations. From the numerical values in Table 1 and the extracted watermarks shown in Fig. 5, one can be seen that λ indeed controls the balance between image quality and robustness. It is clear that the HS values increased and

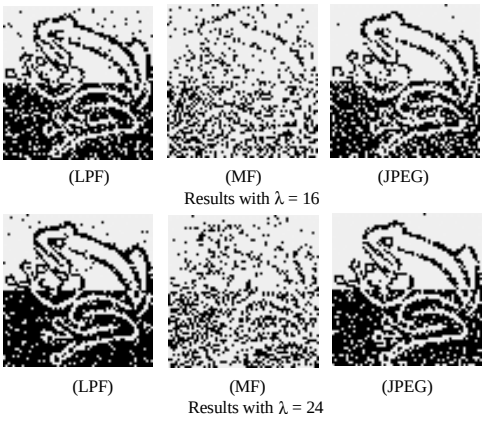

Fig. 5: Comparisons of the extracted watermarks from cameraman

Table 1: Watermarking cameraman with different

λ	Average PSNR (dB)	Average HS (LPF)	Average HS (MF)	Average HS (JPEG 75%)
12	44.30	0.8435	0.6572	0.8357
16	44.27	0.8975	0.6650	0.8718
20	44.08	0.9311	0.6785	0.9001
24	44.02	0.9431	0.6899	0.9172
28	43.92	0.9478	0.6956	0.9246

PSNR decreased by increasing λ from 12 to 20. When the λ value was further increased to 24, the PSNR value reduced a little while the HS values did increase further. Although, the PSNR dropped a little, such drops remain objectively unnoticed. However, by increasing λ to 28, the HS values were slightly increased, while the PSNR values were reduced. According to the tests for all six test images, the average increase of the HS values for LPF, MF and JPEG attacks by adjusting λ from 12 to 24 are 12, 5

Table 2: Experimental results on the test images with different iterations

	Iteration = 1				Iteration = 2			
Results	Average PSNR (dB)	Average HS (LPF)	Average HS(MF)	Average HS (JPEG)	Average PSNR (dB)	Average HS (LPF)	Average HS (MF)	Average HS (JPEG)
Airplane	46.71	0.9571	0.7640	0.9088	47.04	0.9589	0.7708	0.9162
Lena	45.05	0.9745	0.7856	0.9293	45.22	0.9771	0.7924	0.9456
Pepper	45.57	0.9767	0.7842	0.9388	45.92	0.9798	0.7932	0.9524
Baboon	46.24	0.9363	0.7217	0.9697	48.02	0.9407	0.7331	0.9868
Cameraman	43.64	0.9353	0.6716	0.8889	44.02	0.9431	0.6899	0.9172
Goldhill	46.72	0.9802	0.7961	0.9766	47.27	0.9817	0.8005	0.9856

Fig. 6: (a) The original image of Lena and (b) the watermarked image of Lena

and 9.8%, while the average drop in PSNR is 0.6%. Thus, it is suggested that $\lambda = 24$ would be a good compromise between watermarked image quality and robustness.

After determining a suitable value of λ, the hill climbing process of the proposed watermarking method was executed with 1 and 2 iterations. The PSNR of the watermarked image and HS between the original watermark and the extracted watermark is reported and the numerical results are shown in Table 2. As an example, the watermarked Lena image is shown in Fig. 6 and the recovered watermarks under different attacks are shown in Fig. 7, where the hill climbing process was executed by 2 iterations. The algorithm has been tested with more than 2 iterations, however, no obvious improvement was obtained when compared to the results for two iterations. Thus, running the algorithm with two iterations is suggested to be a good compromise for time, efficiency and embedding results.

Subjective quality evaluation of the proposed watermarking method has also been conducted by visual tests involving 10 postgraduate students. All selected students had over two-year experience in image processing and image editing, so that they have a better sense of image quality. A total of six images were used. A watermark (the frog) was embedded into the images by using the proposed method, with $\lambda = 24$ and 2 iterations. The evaluation had two sections and the duration of the observation of each image was 15 seconds. In the first section, participants saw the original and the watermarked image and were asked to report dissimilarities between the two images, using a 5-point impairment scale: (5: imperceptible, 4: perceptible but not annoying, 3: slightly annoying, 2: annoying 1: very annoying). The lowest impairment scale value recorded in this section was 3 and the average Mean Opinion Score (MOS) was 4.6. In the second section, participants were repeatedly presented with original and watermarked images in random order and they were asked to point out which one was the watermarked image (blind watermarking test). A discrimination value close to 50% means that the two images, the original image and the watermarked image, can hardly be discriminated. The discrimination value obtained during the tests with the 6 chosen images ranged from 49 to 58%.

In order to conduct a comparison, a baseline method was carried out, which randomly selects the embedding locations in the middle frequency bands in the DCT blocks. All the tests were executed 30 times on an Intel Core2Duo E8400 CPU with 2G RAM computer. The given Table 3, which compare the average PSNR and HS values of the proposed method, the baseline method and other GA based methods (Shieh *et al*., 2004; Wei *et al*., 2006; Huang *et al*., 2009). The proposed algorithm outperforms the baseline and previous genetic watermarking methods in both image quality and robustness, except in the case of a JPEG attack.

Fig. 7: The images of Lena under different attacks and the extracted watermark, respectively

Shieh *et al.* (2004) and Huang *et al.* (2009) proposed methods having a higher ability to resist the JPEG attack. In general, the time required for embedding a watermark in an image is reduced by 50% to 60%, when compared with the two previous genetic watermarking methods (Wei *et al.*, 2006; Huang *et al.*, 2009) and is 6 times faster than the one proposed by Shieh *et al.* (2004).

The algorithm, with $\lambda = 24$ and 2 iterations, has been tested for some attacks which are not included in the optimization process. The attacks include resizing, Gaussian noise, brightening, darkening and chopping. Again, all the tests were executed 30 times in the same computer. One of the examples, Goldhill after different attacks, is shown in Fig. 8. The extracted watermarks of Goldhill, after suffering from different attacks, are shown in Fig. 9. The average results of the 6 test images are shown in Table 4. According to the table, the proposed algorithm is also robust in regard to those attacks which are not included in the optimization process. It seems that the proposed algorithm tends to resist brightening and darkening attacks inherently. Therefore, in the fourth and fifth columns of Table 4, it can be seen that the HS values after brightening and darkening attacks still have reasonably high levels. The proposed method tends to resist brightening and darkening attacks based on its characteristics. It is suggested that brightening and darkening attacks are not required during the optimization process. Based on the watermarking scheme, algorithm designers and users can choose different attacks for optimization. If one wants to make the algorithm more robust to a certain attack, such as Gaussian noise attack, the attack can simply be added into Eq. 14, namely incorporating it into the optimization process.

Finally, the chosen embedding location histograms of Lena and Pepper after 2 iterations are shown in Fig. 10. It is interesting to observe that for different images, the hill climbing algorithm selects different sets of frequency

Table 3: Comparison with other GA based methods based on Lena

Comparison	Average PSNR (dB)	Average HS (LPF)	Average HS (MF)	Average HS (JPEG 75%)
Proposed algorithm	45.22	0.9771	0.7924	0.9456
Baseline	40.91	0.9313	0.5696	0.7365
Algorithm by Shieh *et al.* (2004)	34.09	0.7101	0.7634	1.00
Algorithm by Wei *et al.* (2006)	42.24	0.8607	0.7723	0.7026
Algorithm by Huang *et al.* (2009)	43.37	0.7033	0.7525	0.9542

Table 4: The results of the extracted watermarks and HS values where the attacks were not considered in the optimization process

Results	Average HS (Resize to 3/4)	Average HS (Gaussian noise)	Average HS (Brighten 20%)	Average HS (Darken 20%)	Average HS (Crop 1/4)
Airplane	0.8372	0.9401	0.9791	0.9867	0.8741
Lena	0.8895	0.9411	0.9954	0.9970	0.8712
Pepper	0.9023	0.9415	0.9826	0.9907	0.8740
Baboon	0.8276	0.9387	0.9905	0.9966	0.8738
Cameraman	0.7588	0.9382	0.9602	0.9694	0.8752
Goldhill	0.9099	0.9438	0.9954	0.9968	0.8582

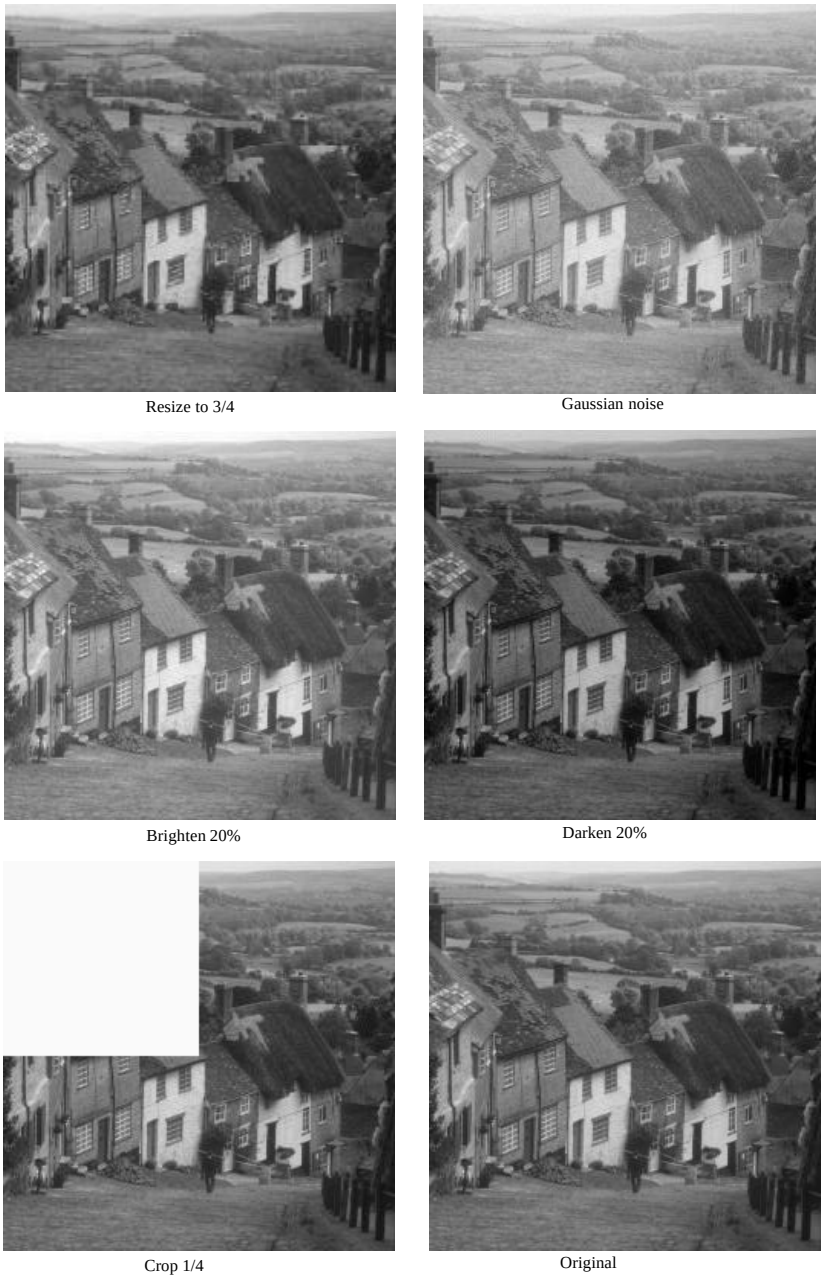

Fig. 8: Extracted watermarks of Goldhill after different attacks

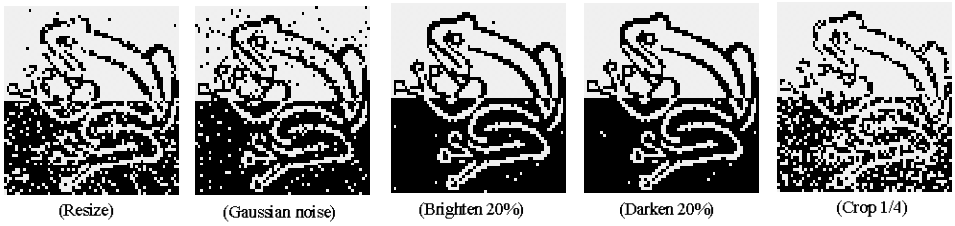

Fig. 9: Extracted watermarks of Goldhill after different attacks

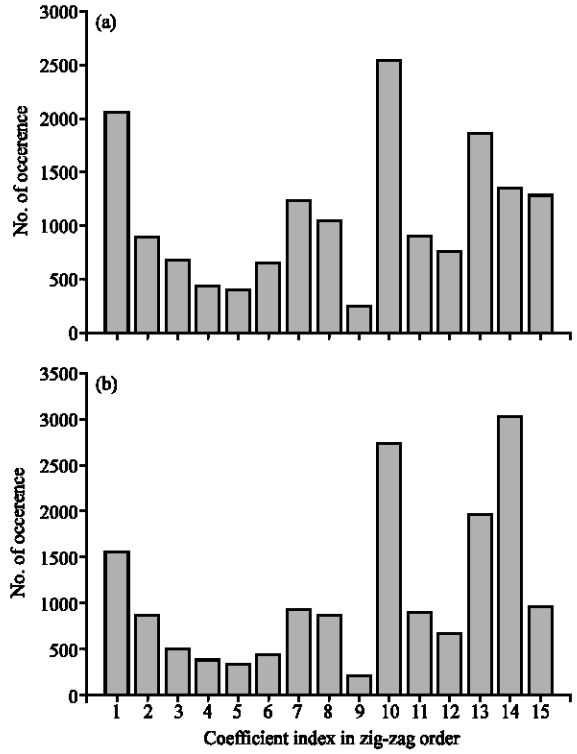

Fig. 10: Different sets of frequency bands selected by the hill climbing algorithm. (a) Pepper and (b) Lena

bands. For the Lena image, most watermark bits are embedded into the higher frequency bands, whilst, for the Pepper image, relatively lower frequency bands are used for embedding the watermark bits. Therefore, the proposed algorithm can adaptively select the appropriate coefficients to embed the watermark according to the nature of the image, in order to keep the optimized imperceptibility and robustness.

CONCLUSIONS

A robust watermarking method for digital images, based on the hill climbing optimization, is presented in this study. It is robust because an optimization algorithm is used to search for the optimal frequency bands for embedding the watermark. Experimental results show that the hill climbing process is simple and more time efficient than the previous genetic watermarking methods. Its uncomplicated operation and effectiveness can solve the drawbacks of the previous optimization-based watermarking methods using GA. The proposed scheme can cope with different kinds of attacks. In addition, the watermark imperceptibility is also improved with the aid of Watson's model. In the subjective quality evaluation, the discrimination value obtained with the 6 testing images ranged from 49 to 58% which means the watermarked image can hardly be discriminated from the original one. Thus, the proposed method can highly preserve the quality of the host image. Experimental results reveal that obvious improvement can be achieved in both robustness and imperceptibility by applying the proposed method. It can be seen that the proposed method is highly applicable for copyright protection and its flexible ad-hoc attack module is directly extendable to cope with a variety of attacks.

In the real situation, the image owner will have the keys beforehand, which must be kept in a secure location. The decoding process will only be conducted by the owner if and only if he or she wants to prove the copyright ownership. However, there are two limitations of the proposed method. The first limitation is that the capacity is fixed and the second is that some kinds of attack, such as a rotation attack, are hard to be incorporated into the optimization process. Although the proposed method is not robust to the rotation attack, the meaning and commercial values of a rotated or a chopped image are usually highly degraded.

ACKNOWLEDGMENTS

Authors wish to thank the Research Committee and the Department of ISE of the HK PolyU for support in this research project. The work described in this study was fully supported by a grant from the HK PolyU (G-YG44). Gratitude is also extended to the Department of IST of the SYSU and Institute of Astronautic Electronic Engineering of the Zhejiang University.

REFERENCES

Chang, C.C., K.F. Hwang and M.S. Hwang, 2002. Robust authentication scheme for protecting copyrights of images and graphics. IEE Proc. Vision Image Signal Process., 149: 43-50.

Chen, B. and G.W. Wornell, 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Trans. Inform. Theory, 47: 1423-1443.

Cox, I.J., M.L. Miller, J.A. Bloom, J. Fridrich and T. Kalker, 2007. Digital Watermarking and Steganography. 2nd Edn., Morgan Kaufmann Publisher, San Fransisco, CA, USA., ISBN: 0-12-372585-2.

Huang, H.C., C.M. Chu and J.S. Pan, 2009. The optimized copyright protection system with genetic watermarking. Soft Comput., 13: 333-343.

Kumsawat, P., K. Attakitmongcol and A. Srikaew, 2005. A new approach for optimization in image watermarking by using genetic algorithms. IEEE Trans. Signal Process., 53: 4707-4719.

Maity, S.P. and M.K. Kundu, 2009. Genetic algorithms for optimality of data hiding in digital images. Soft Comput., 13: 361-373.

Petitcolas, F.A.P., 2000. Watermarking schemes evaluation. IEEE Signal Process., 17: 58-64.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1998. Attacks on copyright marking systems. Lect. Notes Comput. Sci., 1525: 219-239.

Podilchuk, C.I. and W. Zeng, 1998. Image-adaptive watermarking using visual models. IEEE J. Selected Areas Commun., 16: 525-539.

Qi, H., D. Zheng and J. Zhao, 2008. Human visual system based adaptive digital image watermarking. Signal Process., 88: 174-188.

Shen, R.M., Y.G. Fu and H.T. Lu, 2005. A novel image watermarking scheme based on support vector regression. J. Syst. Software, 78: 1-8.

Shieh, C.S., H.C. Huang, F.H. Wang and J.S. Pan, 2004. Genetic watermarking based on transform domain techniques. Pattern Recogn., 37: 555-565.

Wang, Z. and A.C. Bovik, 2002. A universal image quality index. IEEE Sig. Process. Lett., 9: 81-84.

Watson, A.B., 1993. DCT quantization matrices visually optimized for individual images. Proceedings of the SPIE International Conference Human Vision, Visual Processing and Digital Display, Feb. 01, San Jose, CA, USA., pp: 202-216.

Wei, Z.C., J.F. Dai and J.X. Li, 2006. Genetic watermarking based on DCT domain techniques. Proceedings of the IEEE CCECE/CCGEI, May 7-10, Ottawa, Canada, pp: 2365-2368.